DEVELOPMENT OF WIRELESS NETWORK SYSTEM ON A POWER WHEELCHAIR

A thesis submitted in partial fulfilment of the requirements for

Master of Mechanical Engineering

at the University of Canterbury

by Yiwei Hu

University of Canterbury

2012

ABSTRACT

The development of wireless communication technology offers new opportunities to enhance the functionalities of mobility systems (e.g. powers wheelchairs and robots). This thesis presents new hardware and software architecture to offer ease of user control and power efficiency to an autonomous mobility system by using Wireless Networked Control (WSC). A wireless network is applied to perform both environment sensing and user control. The development will be demonstrated through a case study on a power wheelchair.

The challenge in the development of such a wireless solution is to accomplish a set of system activities (e.g. system initialization, system monitoring, power management) under different circumstances within a dynamic wireless network without sacrificing flexibility, energy-efficiency, or reliability.

The optimal way to achieve this is to design a protocol stack orientated to the demand of a specific system with cross-layer optimization. However, it requires significant design effort. In this thesis, a wireless network is constructed by utilizing a commercial-of-the-shelf (COTS) protocol. The development focuses on system integration and Application Layer. This accelerates the development progress with the benefits of cost effectiveness and less burden on protocol design. However, the COTS protocol is not able to provide a solution with maximum efficiency, because that the development of a COTS protocol is constrained by many factors. For example, the low layers of a COTS protocol are usually not available for customization due to the license issue.

The aim of this project is to develop a wireless platform to enable wireless functional devices to be added into a mobile system. The main benefit of such a wireless network system (WNS) is to allow new modules to be readily incorporated into the mobility system, which otherwise are difficult, because either, the physical wiring is prohibitive or the current system does not allow the signals to be processed.

The strategy for developing such a wireless network with desired functionalities is to build both identity management module and power management module based upon system design and Application Layer development. The identity management module allows the system to perform self-construction and self-maintenance and the power management offers high power efficiency. These two modules are developed independently and integrated into an autonomous control loop. Transitions between different modules are achieved by handshaking protocols. The advantage of such a strategy is the ease for customization and extension. The infrastructure includes gateway, Log-in system and radio frequency (RF) platform.

ACKNOWLEDGEMENTS

To begin, I suppose the first person to acknowledge would be Ian Palmer, my project mentor from Dynamic Controls Ltd. While I did my internship in Dynamic Controls Ltd, he encouraged me to apply graduate studies. Thanks for his assistance in preparing all the documents for TIF funding applications, making this project possible, and the support he gave along the project development, not only helping me in building the project plan and assuring the project is correctly orientated, but more importantly, familiarizing me in industry environments. I am pretty sure I will benefit from the experiences in working with him for the future career perspective. His enthusiasm and his patience and calm determination helped me through the frustrating times I have suffered while I was disoriented in this new research area.

Foremost, I would like to thank my supervisor Dr. XiaoQi, Chen from the department of Mechanical Engineering and Dr. Allan McInnes from the department of Electrical Engineering. Their invaluable knowledge leads me up the right path of academic research, making my work much more easily than it may have.

I am grateful to work in the Wireless Research Centre (WRC) group in NZi3, for the fantastic facilities provided and its joyful environment. Thanks to Jeremy Reece, who was the manager of WRC, I still remembered that he spent a whole morning to teach me the methodologies for academic research. And my thanks also to Graeme Woodward, the research leader in WRC, who is the most hardworking people I have ever seen. His enthusiasm is always contagious and inspiring.

Finally, I appreciate Foundation for Research, Science & Technology and Dynamic Controls Ltd for the research funding they provided for the research so that I am able to complete the full time component of my enrolment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

AOA	Angle of Arrival
BCS	Battery Charge Station
COTS	Commercial off The Shelf
GPS	Global Position System
GUI	Graphic User Interface
JTAG	Joint Test Action Group
LDM	Location Discovery Module
MCU	Microcontroller Unit
MSS	Master Slave Swap
MTR	Mechanical Transfer Robot
NFC	Near Field Communication
OOB	Out of Band
PIN	Personal Identification Number
QoS	Quality of Service
RF	Radio Frequency
RSS	Received Signal Strength
RSSI	Received Signal Strength Identification
SPI	Serial Port Interface
SNR	Signal-to-Noise Ratio
TDMA	Time Division Multiple Access
TDOA	Time Difference of the Arrival
TOA	Time of Arrival
WSC	Wireless Networked Control

WNS	Wireless Network System
WSN	Wireless Sensor Network

Chapter 1 INTRODUCTION

In recent years, due to the development of wireless communication technologies, wireless network systems (WNS) have become an exciting area of research. Information is exchanged among sensors, actuators, and controllers over a wireless network. Wireless communication has been an enabling technology for many military, industrial and commercial applications, allowing fast deployment, flexible installation, fully mobility and avoiding wear and tear problem due to cables.

This thesis presents the architecture design of a wireless network that builds wireless links between stationary components within a mobility assistive device, and works as a complement to a wired network (e.g. CAN Bus). The performance will be demonstrated through case studies and test beds in a power wheelchair.

Networked control provides a real time capacity to exchange information between sensors and actuators in a closed control loop. With advancements of wireless technology, wireless platforms can be integrated into the existing networked control systems, such as ARINC 629 in avionics, TCN in trains and CAN Bus in cars and power wheelchair. The wireless networked control takes advantages based on mobility, ease of installation and maintenance. However, wireless communication is error prone and power constrained compared with wired communication. This research work aims to develop a wireless networking prototype which is intended to interface with the existing CAN Bus back bone to enhance the functionalities of a power wheelchair.

1.1 Motivations and Opportunities of Wireless Solutions on a Power Wheelchair

This section presents the motivations for developing a wireless platform to perform control and sensing on a power wheelchair and how the wheelchair system will benefit from it.

1.1.1 Easier Installation and Deployment

Figure 1-1 shows the view of rear of the wheelchair. As more and more functional modules are added into the system, physical wiring becomes a major challenge for engineering and installation. Incorporating wireless communication technology into a networked control system can free the system design from hardwiring. This will offer more space for new functional modules to be installed into the system and allow new modules to be deployed into the positions which are not accessible by hardwiring, e.g. rotating machinery, hazardous or space restricted areas.

Figure 1-1 Rear of a power wheelchair.

For wired infrastructure, the number of devices to be installed is limited by hardware, e.g. number of ports, wiring space and structure obstacles. The applications of wireless technologies can overcome these problems, making design and implementation much easier.

1.1.2 Runtime Adaption

Wireless technology offers greater flexibility. The nature of a wireless network enables it to maintain performance in the presence of node, link and topology changes. Ease of runtime expansion allows new devices to be added into the system through wireless pairing with simplicity. On the contrary, for a wired system, the cost to modify infrastructure is usually much higher and continues to increase.

Figure 1-2 Fast deployment on a power wheelchair.

As shown in Figure 1-2, a pressure field sensor is required to be installed into a wireless network on a power wheelchair system for monitoring the pressure on headrest. The sensor node is able to join the network by a serial of handshaking procedure to achieve automatic network construction, without need of hardware configuration or user interventions. In

contrast, for a wired network, physical device adaption and configuration may be involved to achieve this purpose. For example, a socket may require more ports to support the connections and firmware needs to be updated to discover such a new device.

1.1.3 Mobility and Transfer Aid

Wireless control also offers better mobility. For instance, through wireless remote control units, users could park the wheelchair remotely before sleep and drive the wheelchair back to a position near the bed through remote control. This could provide for the ability to transfer between wheelchair and bed without other human assistance in some circumstanses. This also helps the users to drive the wheelchair remotely to a predefined docking position for autonomous battery charging. Some mechanical and navigation systems may be involved to achieve the autonomous transferring and battery charging. Figure 1-3 and Figure 1-3 show the Battery Charging Station (BCS) and the Mechanical Transfer Robot (MTR) which are presented in [43].

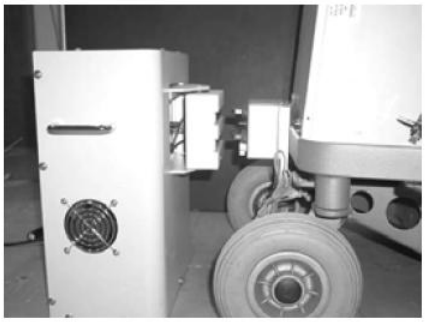


Figure 1-3 Battery charging station.

Figure 1-4 Mechanical transfer robot.

1.1.4 Lower Costs

Wireless technology can lower costs. The cost of commercial RF chipsets is falling due to the rapid development of wireless technology and the growth of the wireless semiconductor industry. However, for wired systems, the cost of wires and connectors can be relatively expensive. Maintenance cost of wires and connectors can be a major concern due to vulnerabilities associated with wear and tear.

1.1.5 Ubiquitous Computing

Wireless networking is an enabling technique which offers a wide range of access for information exchanged between a power wheelchair and other wireless devices such as home computer, Bluetooth cell phone, universal remote control on home appliances (e.g. air

conditioner, TV set and desktop) and wireless environmental control units (e.g. door, window and curtain). This allows a power wheelchair to achieve:

- **Secondary Control**: Many other wireless devices may be incorporated in the wireless network of the wheelchair to perform secondary control. This takes advantages of existing commercial techniques for enhancing the functionalities of the wheelchair controls such as multi-touch screen technique of iTouch and GPS applications on iPhone.
- **Environmental control**: Users are able to remotely control various home devices. This offers the disabled people access for hands-free control in the immediate surroundings via wireless links. A home automation system can be constructed by interconnecting the wireless network and surrounding environment.

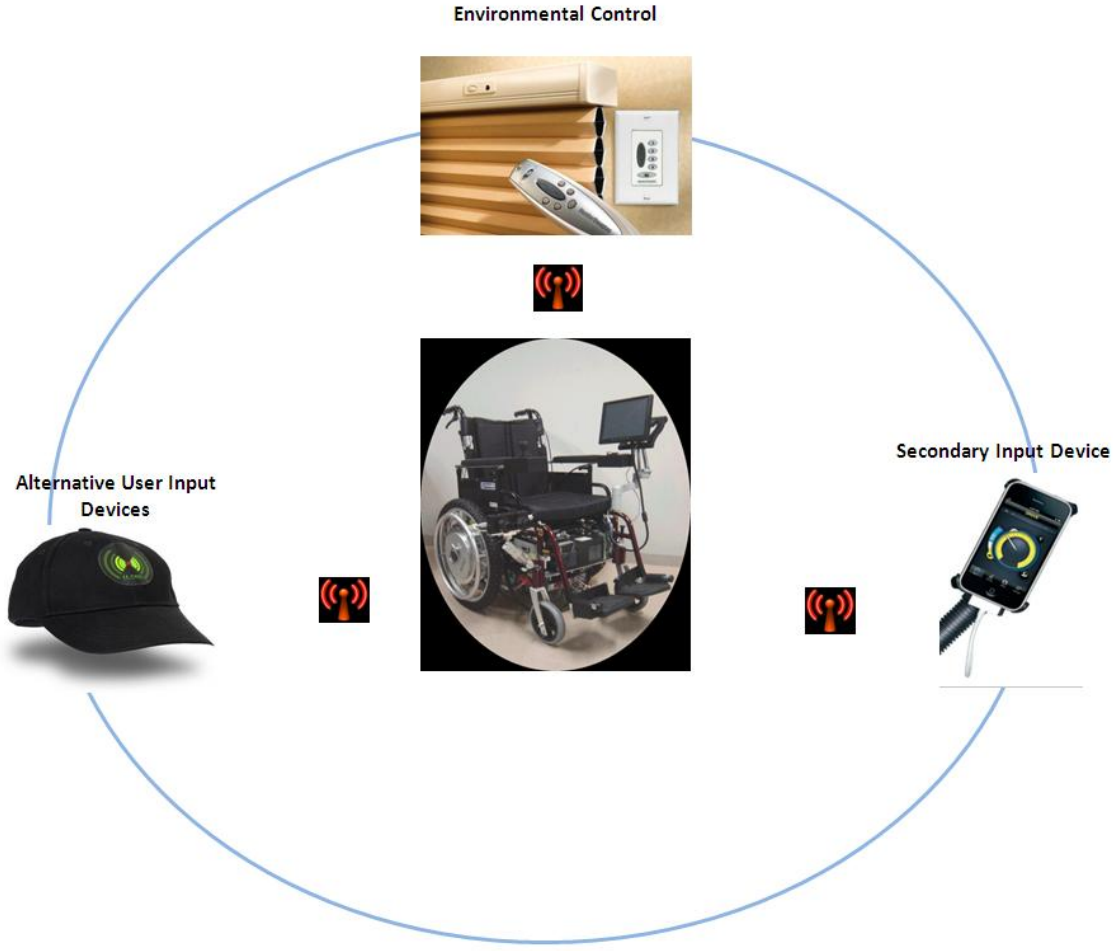


Figure 1-5 Concept design of ubiquitous computing for power wheelchair

As shown in Figure 1-5, the environmental control technology can be employed onto a power wheelchair to facilitate the disables. Secondary input devices employ commercial products such as iPhone and can be achieved by developing applications in Apple's iOS. Many commercial

products have built-in RF solution, such as Bluetooth, allowing wireless connection to the wheelchair to achieve fast deployment and flexibility.

The rapid development of wireless technologies offers great opportunities for ubiquitous computing applications. The wireless applications on a power wheelchair also enable disabled people to improve their quality of lives through ubiquitous computing. Many research works are undertaken in this field [44].

1.2 Thesis Structure

This thesis presents a prototype to demonstrate wireless networked control on a power wheelchair. Various types of sensors and control units will be interfaced and operated with the wireless platform to construct a secure private wireless network on a power wheelchair. This wireless network is developed based on a commercial-off-the-shelf (COTS) protocol.

The main contributions of this work are:

1. A general architecture that meets the requirements of wireless applications on a power wheelchair;
2. An ID management system to enable self-construction and self–maintenance for a Wireless Sensor Network (WSN);
3. A novel power management system for wireless applications on a power wheelchair;
4. A demonstration of a prototype for driving the wheelchair.

This thesis is organized as follows. Following Chapter 1 introduction, Chapter 2 describes application domains of WSNs, and the key factors for designing a WSN. This provides the background for a general understanding of the issues discussed in later chapters. Chapter 3 presents an overview of the system development, including system architecture, protocol selection and hardware design. Chapter 4 describes how to enable the wireless network to perform self-construction and maintenance. Concepts of auto device pairing, device localization and log-in table are introduced. Chapter 5 discusses the power management of the system. A mathematical model is built for power consumption analysis. Finally Chapter 6 concludes the thesis.

Chapter 2 LITERATURE REVIEWS OF WIRELESS SENSOR AND CONTROL NETWORK SYSTEM

A WSN combines sensing, embedded computing, information distribution processing and wireless communication into a single tiny device to perform monitoring, control and actuation tasks. A WSN system is usually composed of a large number of nodes that are deployed densely to collect data from the surrounding, control actuators in the network and take commands from users. A WSN features fast deployment, low power and flexibility compared with traditional wired systems and is favored in many application domains, such as military surveillance, home automation and industry process control. Figure 2-1 shows a home application example, a user is able to control home appliances through a PDA and read measurements of a smoke sensor on the PDA.

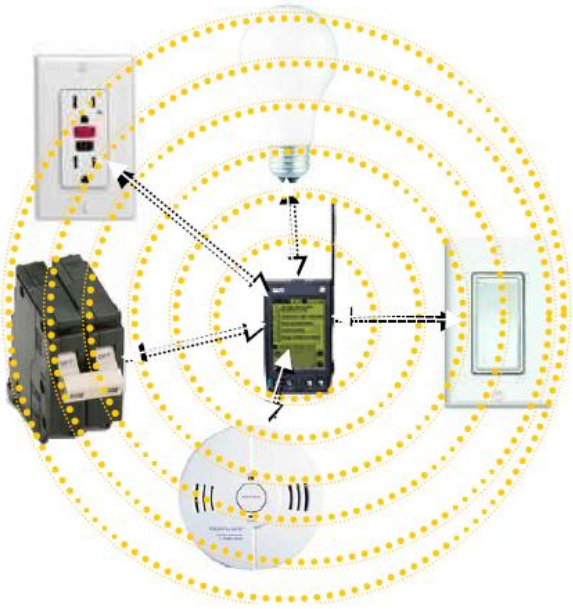


Figure 2-1 Home automation sensors and control network [79].

The continuous advances in integrated circuitry technology have enabled the wireless network sensor node continue to be smaller and cheaper, and have longer lifetime such as the one shown in Figure 2-2. The cost of a wireless sensor node has been reduced to less than $1 and the vision is that the cost will continue to decease [55].

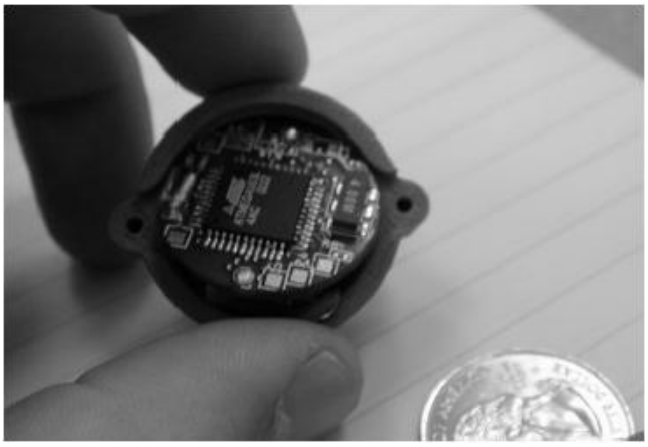


Figure 2-2 DOT – WSN device designed to be the approximate size of a quarter [55].

Many researchers have been engaged into this research area to extend the applications of the wireless network systems in the industry, military and agriculture areas. These applications cover many different domains to perform tasks of surveillance and detection, process monitoring and control, localization and tracking. This enables fast deployment, ease of maintenance, low cost, protecting operators from working in hazardous environments or frees operators from the burden of intensive duplicated operations. Many research works have been studied in recent years and part of them are summarized in Table 1 [45].

Area	Applications
Industrial	Monitoring and control of industrial equipment (LR-WPAN) [46].
	Factory processes control and industrial automation [47].
	Manufacturing monitoring [48].
Military	Military situation awareness [47].
	Sensing intruders on bases, detection of enemy units movements on land/sea, chemical and biological threats and offering logistics in urban warfare [49].
	Command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems [50].
Mobile wireless low-rate networks for location physical world	Tracking of assets, people, or anything that can move in various environments, including industrial, retail, hospital, residential, and office environments, while maintaining low-rate data communications for monitoring, messaging, and control [46]. Monitor and control the physical world: deployment of densely distributed sensor/actuator networks for a wide range of biological and environmental

	monitoring applications, from marine to soil and atmospheric contexts; observation of biological, environmental, and artificial systems; environmental monitoring of water and soil, tagging small animals unobtrusively, and tagging small and lightweight objects in a factory or hospital setting [51].
Public safety	Sensing and location determination at disaster sites [46,52]
Airports	Smart badges and tags [46, 52]. Wireless luggage tags [46]. Passive mobility (e.g., attached to a moving object not under the control of the sensor node) [53].
Automotive	Tire pressure monitoring [46, 52]. Active mobility [53]. Coordinated vehicle tracking [47].
Agriculture	Sensing of soil moisture, pesticide, herbicide, pH levels [46, 52].
Emergency situations	Hazardous chemical levels and fires (petroleum sector) [46]. Fire/water detectors [49]. Monitoring disaster areas [50].
Rotating machinery	Monitoring and maintenance (electric sector) [46].
Commercial	Managing inventory, monitoring product quality [48, 50].
Medical/ Health	Monitoring people's locations and health conditions [48]. Sensors for: blood flow, respiratory rate, ECG (Electrocardiogram), pulse oxymeter, blood pressure, and oxygen measurement [54]. Monitor patients and assist disabled patients [50].
Ocean	Monitoring fish [48].

Table 1 Applications for wireless sensor and control network.

The design of wireless sensor and control network is highly application-dependent due to the requirements differing from one application to another, which results in different design strategies. To design a WSN for some particular applications, it is primarily to define the requirements and evaluation metrics to measure the success of the design [53, 55]. These evaluation metrics are explicitly considered as dimensions in the design space. The evaluation metrics can be categorized into system level and device level. The system level evaluation focuses on system performance, such as coverage, security, accuracy and etc. while the node device level evaluation underlines software and hardware design for individual node. The descriptions are listed in Table 2 and Table 3 respectively:

Level	Domains	Description
System Evaluation Metrics	Lifetime	The expected lifetime of a WSN is limited by the energy supply, transmission output power and radio duty cycle.
	Coverage	Coverage refers to the physical area a network covers. It is tied to scalability of a network to extend from a small trial network to a large scale network to support large number of nodes.
	Cost	In a long term, the total cost for a wireless network system has more to do with the maintenance. The system needs to be robust and capable of performing continual self-maintenance to reduce cost.
	Ease of deployment	A wireless network system should be capable of assembling itself and adapt itself to changing conditions. This requires it automatically configure itself.
	Response time	It is critical for applications relevant to control purpose. However, a trade-off between response time and lifetime needs to be taken into account.
	Temporal accuracy	A network must be capable of maintaining a global time base that can be used to aggregate collected data to achieve temporal accuracy.
	Security	A combination of privacy and authentication is required to keep the security of a system. However, use of encryption and cryptographic authentication cost more power and bandwidth.
	Effective sample rate	This refers to the rate that a system collects data from surroundings and report data to an access point.

Table 2 Network system evaluation metrics [53], [55].

Individual Node Evaluation Metrics	Power	Wireless node requires both low-power hardware components and low-duty cycle operation techniques. Power harvesting components is another option and very expensive.
	Flexibility	A node must be flexible and adaptive to work with a wide range of scenarios with different demanding of applications.
	Robustness	Robustness refers to hardware robustness and coexistence with external interference. Hardware robustness requires hardware design with modularity methodology. Multi-channel and spread spectrum radios can greatly increase the robustness of wireless links.
	Security	A node needs a CPU that can handle cryptographic operations to perform complex encrypting and authentication algorithms.
	Communication	This refers to communication transceiver capability with communication rate, power and range, which are determined by the design of RF hardware platform.
	Time Synchronization	Node must be able to maintain precise time synchronization with other nodes in the network to perform data aggregation and device cooperation. Clock drifting of timekeeping hardware must be overcome to achieve it.
	Size and cost	The physical size and cost of each individual node has a large impact on node deployment and commercial applications, this must be considered while the initial stage of hardware design.

Table 3 Individual node evaluation metrics [53], [55].

Table 2 and Table 3 briefly describe some factors in both system evaluation metrics and node evaluation metrics. These factors determine the system performance at different levels and can be achieved by taking advantages of researches result in wireless technologies, wireless protocol, system integration and services. This will be described in Section 2.1.

This chapter has been organized into two sections: Section 1 introduces factors which have influence on wireless sensor and control network; Section 2 focuses on some particular applications of wireless sensor and control network systems and briefly describe how the design strategies are applied in such projects.

2.1 Design Space on Wireless Sensor and Control Network Design

We have discussed the evaluation metrics to measure the performance of a WSN system. However, to achieve the desired requirements, we need be aware of the design dimensions which have an impact on system performance. These research issues can be classified into three groups: system, protocol and services, as shown in Figure 2-3.

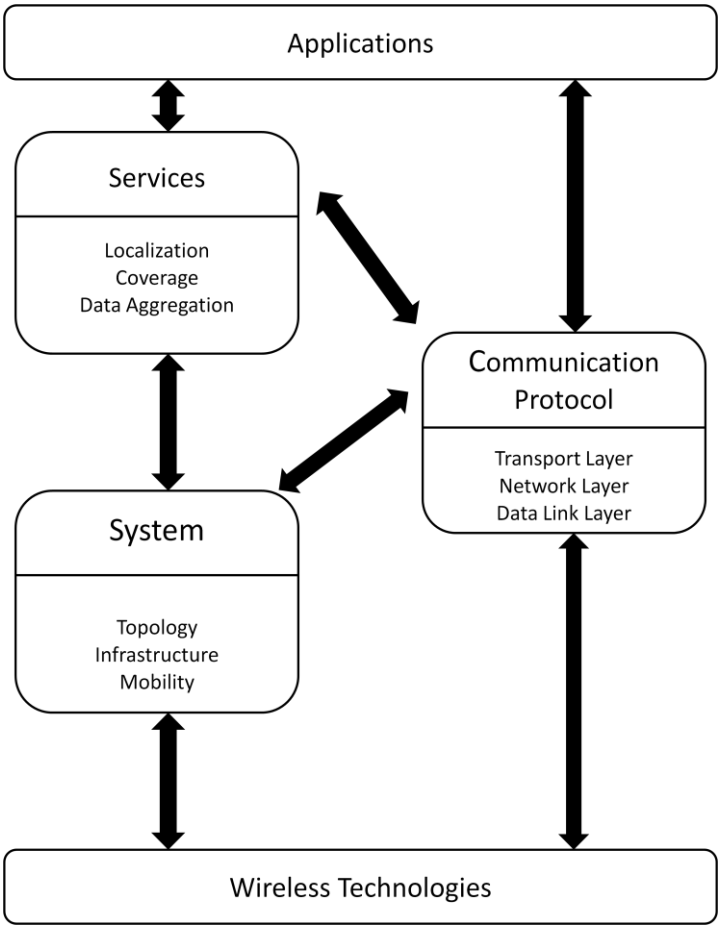


Figure 2-3 Broad classification of various issues in a WSN.

In this section, these key factors for developing WSNs will be discussed in detail to provide a context for later chapters.

2.1.1 System

In Figure 2-3, the first group to be introduced is the system. Each WSN is an individual system, which integrates multiple wireless devices into a network to achieve desired functionalities. System integration may vary due to the requirements of system mobility, heterogeneity, network topology and hardware and software support.

Mobility

Mobility of a wireless network may refer to the change of location of individual nodes in the run-time. Mobility may be designed by purpose to perform some desired tasks (e.g. environmental sensing) or it may occur due to unexpected incidents (e.g. environmental change). Mobility can also be a property of the entire system. For example, a wireless network is carried by an automotive system [53]. Mobility can be defined by measure of degrees, in terms of frequency, speed and time periods of its occurrence. Mobility has a large influence on the design of protocols and algorithms of a wireless network. The network may have to change topology dynamically during the run-time, participating nodes in the network need to search for optimal routing to forward messages according to the change of topology automatically.

Heterogeneity

A WSN is a heterogeneous system that is capable of performing different tasks with a variety of devices. Unlike a homogeneous network system that consists of identical devices, nodes may differ in requirements such as message rate, hardware components and computational capacity in a heterogeneous system. A wireless network with high degree of heterogeneity will require the system to manage individual nodes with different configurations, which will increase the complexity of the communication protocol in terms of channel management, power management and device management.

Infrastructure

The various wireless communication modalities can be used to build a communication network system. Two common forms of architecture are infrastructure-based networks or base station mode, ad-hoc networks.

In infrastructure-based networks, sensor nodes construct the network in a predefined architecture, and communications between nodes rely on a base station. An example is shown in Figure 2-4. Communications between two nodes are only allowed to be exchanged via a base station.

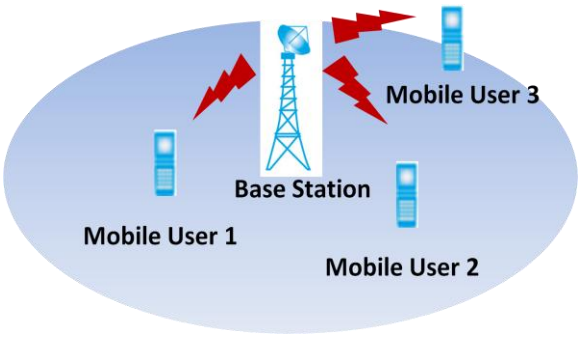


Figure 2-4 Infrastructure-based network.

In ad-hoc networks, wireless communication does not rely on an existing infrastructure. Instead, any node in the network is able to act as a router or access point to forward messages for other node. An ad-hoc network offers flexibility for participating nodes to dynamically change the messages routing due to the connectivity of the network. An example is shown in Figure 2-5. Ad-hoc networks features ease of deployment, flexibility and robustness in the presence of dynamic changes. However, they rely on routing algorithm, which increases complexity and intensity of networking communication.

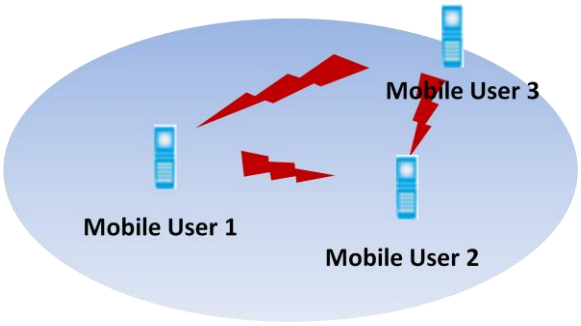


Figure 2-5 Ad hoc Network.

A hybrid network may be used for some applications, which combines both ad hoc networks and infrastructure. With such infrastructure, wireless nodes within a cluster interconnect with each other based on ad-hoc infrastructure, and several clusters forms an infrastructure-based network.

Network Topology

Network topology is the actual geometric pattern of interconnection between all wireless nodes in a network. Network topology can be either physical topology or logical topology. Physical topology refers to the physical location, devices and installation, whereas, logical topology refers to the path that data transferred in the network from one node to another or the relative location of each node. Some basic network topologies are shown in Figure 2-6.

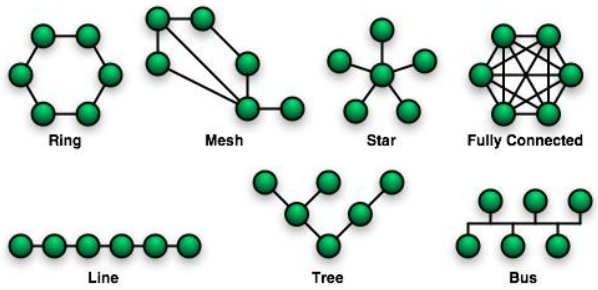


Figure 2-6 Network topologies [56].

Network topology affects the characteristics of a network system in many different ways as latency, robustness and capacity. The routing algorithm and network protocol also rely on the network topology.

2.1.2 Communication Protocol

Network protocol is the predefined rule for network to format digits and exchange data between nodes. It provides software support and enables the network to perform signaling, routing, authentication and error detection and correction. Network protocol is build upon an ISO-OSI (International Standards Organization – Open Systems Interconnection) Reference Model with a layered structure, firstly proposed in [57]. This reference model is composed of seven layers, with particular functions for each layer, as shown in Figure 2-7.

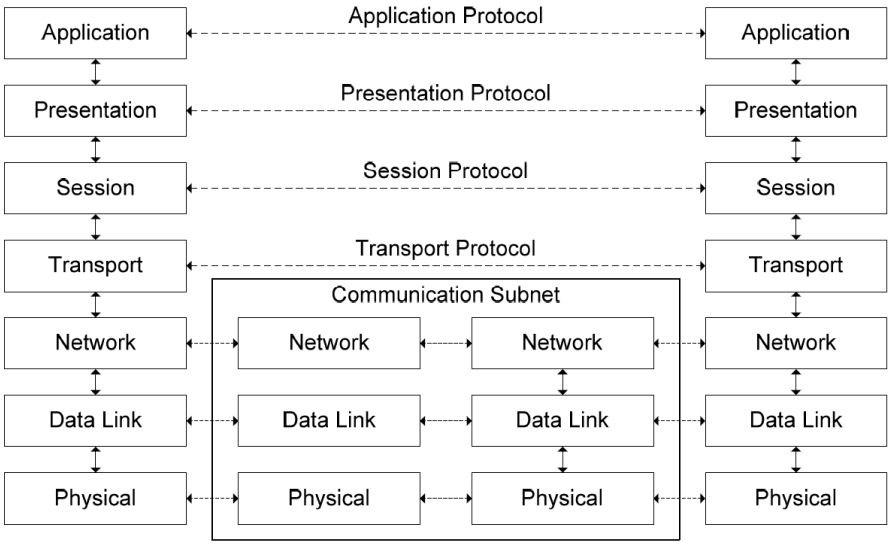


Figure 2-7 The ISO-OSI reference model.

The layered structure simplifies the design of the network protocol by separating the communications into logical smaller components. This offers flexibility for development of new protocol by adding new protocol stacks or network service modules to an existing layered architecture.

The upper layers of the ISO-OSI model, including Application Layer, Presentation Layer and Session Layer are designated for application-specific functions, such as data formatting, encryption and connection management.

The remaining lower layers of the ISO-OSI model, however, provide more primitive network-specific functions as foundation for networking, routing algorithm, and addressing and flow control.

In contrast to traditional wireless networks, to date there is no standardized protocol for WSNs. Many commercial companies establish their protocol stacks with different architectures. For example, the ANT protocol utilizes a five-layer protocol structure, as shown in Figure 2-8, some layers (Network Layer and Transport Layer, Presentation Layer and Application Layer) in the ISO-OSI model are merged into one layer and Session Layer is eliminated to achieve simplicity and power-efficiency in this case.

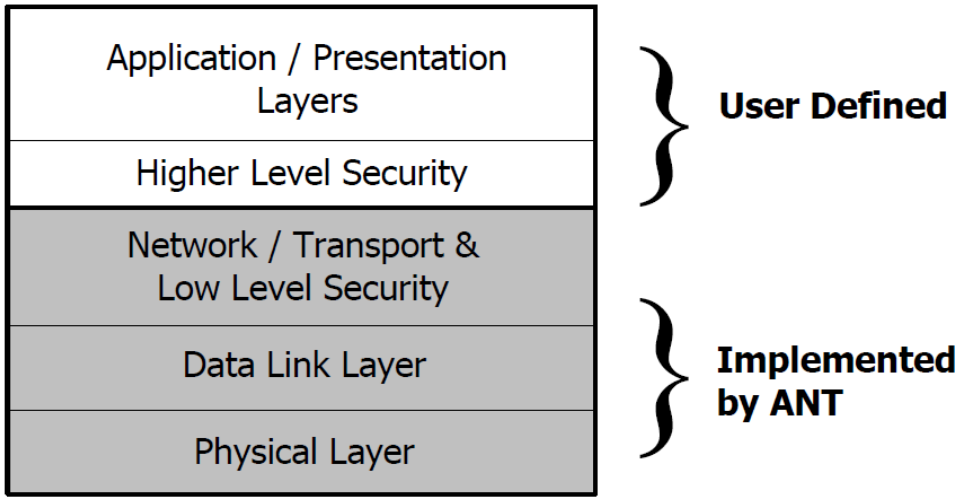


Figure 2-8 ANT layered structural protocol [93].

A wireless network system can be optimized by adapting the network protocol to a specific particular application domain. Intensive efforts have been spent on protocol optimization for WSNs, to meet the particular requirements such as low-power, scalability, node mobility and etc.[58, 59].

2.1.3 Service

Service can be evaluated by Quality-of-Service (QoS), which is determined by communication protocol and system platform. QoS measures the performances of a wireless system in terms of its functionalities, such as localization, system latency, data aggregation and etc. It is an outcome of the design of system and protocol.

Real Time

In some particular applications such as surveillance and control applications, the system is required to provide real-time service to update information with quick response time. The real-time property requires the system to keep tracking the environmental change all the time, which is usually power-consuming. To achieve real-time performance without sacrificing power efficiency, a low-power preprocessor (or event generator) can be employed to monitor the environment, triggering wireless communication while critical events are detected and forwarding the messages down a dedicated communication channel.

Coverage

Coverage of a wireless network measures the physical area that the wireless communication of a network covers. For an infrastructure-based network, the coverage depends on the transmission range of the base station. However, for an ad-hoc network, the multi-hop communication technique can extend the coverage of the network. The requirements of network coverage are application-specific, thus, for deploying a wireless network, its scalability is very important to be taken into account for applying the network in different applications, allowing the wireless network to be deployed either in small trial network or extended to a large size to meet the requirements. This property may require proper protocol and system design.

Data Aggregation

The main purpose for data aggregation algorithms is to gather information of surroundings which are collected from multiple small wireless device nodes in the network and synthesize the information for analysis and operations. Another advantage for data aggregation is to enhance the lifetime of the nodes which are battery-driven, as the data will be aggregated in a cluster of closely deployed nodes with power efficiency to reduce the amount of data needed to be transmitted to a base station or sink. This is an effective approach especially for a large-scale network. Data aggregation algorithm is highly dependent on the network topology and infrastructure, and it is usually coupled with network protocols for medium access control (MAC). Many different data aggregation approaches can be found in [99].

2.2 Summary

Wireless sensor and control networking has been envisioned as an emerging technology and a wide range of applications will integrate it into our lives in the future. There have been intensive efforts on protocol optimization for satisfying the specifications of wireless sensor and control network system applications [75], [76], [77]. These research themes have different focuses or use different techniques, to adapt existing wireless communication protocol stack to WSN systems as the wireless protocols for WSN pose a number of unique challenges, due to the following factors:

1. **Hardware constraints**: Sensor nodes are very limited in power, computational capacities and memory.
2. **Dynamic changes**: It is required that the sensor nodes must be able adapt to frequently changing connectivity as well as environmental stimuli.
3. **Unattended operations**: In many cases, once the sensor nodes deployed, little human intervention will be possible. Hence, the network system needs to do configuration, maintenance and diagnosis by themselves.
4. **Ease of deployment**: Sensor nodes are usually densely deployed in large numbers without any predefined infrastructure. In this situation, it is up to each node to automatically identify its connectivity and distribution and assemble the network.
5. **Node identification**: Sensor nodes may not have global identification to reduce the amount of overheads. This may pose problems for network construction.

However, realization of WSN needs to satisfy many constraints due to the nature of wireless communications and architecture of wireless network, such as error rate, power consumption, run-time topology change, scalability and etc. Many researchers have been engaged into in developing the technologies of wireless sensor and control network to meet requirements in different applications domains. These research projects can be categorized into two types: protocol-oriented and system-oriented. Protocol-oriented projects focus on developing communication protocols to optimize WSN performance in some dimensions e.g. power consumption error detection and correction and etc. System-oriented projects target to some particular applications and provide solutions and achieve performance optimization by system integration.

The importance of these challenges may vary in different applications. For example, energy-efficiency may be a primary factor if scattered remote nodes are powered by a battery which is not replaceable or rechargeable and requiring up to years' operation without human interventions. On the other hand, this factor may be sacrificed for some other applications, for example, critical control on industry process requiring high data rate and high reliability. For

such applications, the system can apply redundancy to enhance the reliability, hence consumes more power.

There have been many wireless sensor and control network applications undertaken with various communication protocols and system designs for adapting wireless network systems to different environmental conditions. In this thesis, we present a wireless sensing and control system to achieve low-power, ease of installation and implementation of such a prototype system to enhance the existing wired wheelchair system.

Chapter 3 System Overview and Hardware Design

We present some general discussions for constructing a wireless control network over a mobility system in previous sections. In this chapter, we will focus on a case study to demonstrate our design strategy.

We propose to build protocol architecture to realize wireless networked control on a power wheelchair. Different types of user input devices are involved in system demonstration. The types of wireless input devices are as follows:

- Switch inputs for seating, lighting, specialty switch inputs
- Secondary proportional joystick control
- Auxiliary Input Modules such as Attendant control units

Our target is to interface these devices with an RF platform and implement them wirelessly. These wireless devices will work as a complement to existing wired system through a gateway node. The gateway node has both wired and wireless links, and it operates as a wireless base station to coordinate the wireless network.

The intent on this project is to provide a wireless protocol that can be embedded into final commercial products and a hardware template that is capable of incorporating the wide range of devices envisioned for the future by running the designed protocol. Our strategy is based on the development of a COTS protocol stack to realize application optimization. In general, this includes optimization over Physical Layer to Application Layer, individually (e.g. suboptimal network design) or jointly (e.g. cross-layer optimization). However, it will be very time-consuming and workload-intensive to achieve optimization through multiple layers. In this project, we will focus on development of Application Layer.

The proposed research is organized in 3 work-packages (WP). In WP1, a COTS RF technology will be selected which will match the requirements of wireless applications on a power wheelchair. WP2 studies the architecture of the prototype. WP3 concerns issues mainly associated with the hardware design.

3.1 Protocol Selection

With the statements present in Section 3.1, the existing protocols and their functionalities for a) control of functions that might cause injury, b) control of environmental functions, and c) audible communication via wireless devices are reviewed. One of them will be selected for applications to perform sensing and control on a power wheelchair.

3.1.1 ANT™ Protocol

ANT™ is a light-weight, low-power 2.4 GHz wireless protocol designed for simplicity and efficiency. The key features of ANT™ are: bi-directional, time division multiplexed, 32 byte protocol intended for low power infrequent communication. ANT™ is commonly used for sensor reporting where critical timing is not an issue. No testing of communication latency has been found which would assure the potential user that adequate safety would be available for critical control functions. Of note is that ANT™ is now commonly utilized in health and fitness applications, including installation in athletic shoes, bicycles, and other similar devices, and the expansion in network size leads to the likelihood of increased latency in communication. ANT™ has not been recommended as a critical control application; but is ideally suited for monitoring functions that are not critical or where instancy of communication is not an issue. ANT™ is primarily a consumer device protocol for low bandwidth, low criticality, low power, long battery life applications.

ANT can be operated in burst, broadcast, or acknowledged modality. Of the three, only acknowledged modality is suitable for control functions, since reliable receipt of control messages would be required to assure low power and high reliability, the other two modes can be used for sensing and monitoring applications. While some progress has been made in reducing latency, ANT protocol now utilizes a randomized Time Division Multiple Access (TDMA) approach to attempt to assure communication throughput. Thus, combined with its low power output and intended range (1 mini-Watt output power, intended for 1 meter range), it is susceptible to interference from nearby sources such as wireless phones Wi-Fi hubs, etc.

ANT is an inexpensive and low-power RF solution which ideally suits the demand of WSNs. It supports up to years operations without replacing or recharging the battery compared with competing “low power” RF technologies which support only months node lifetime in similar applications with similar usage pattern.

ANT is a light-weighted protocol, only requires less than one kByte of resources of host MCU, which is an order of magnitude smaller than competing protocols. As a consequence, it requires less powerful, inexpensive host MCU for driving the protocol, which reduces system costs up to 60 percents.

ANT employs advanced power management pattern, allowing the radio to spend most of time in low-power (consuming just micro-amps) mode and quickly wake up to active mode while

events are detected and then rapidly return to low-power mode when processing jobs are completed. Typical duty cycles (the ratio of transmit and receive time to low-power time) for WSNs are less than one percent, thus the average current consumption remains to be in micro-amp range.

Where long battery life is of the essence, communication range is limited and critical response is not significant, ANT is a very viable, low-cost solution.

3.1.2 Bluetooth™

Bluetooth is an industry standard widely used consumer targeted protocol for wide-bandwidth applications. Bluetooth has been widely deployed in short range communications including cameras, wide-band modems, printers, and wireless audio communications and interface devices. It has been employed in home health monitors, critical health monitoring devices and is found included in virtually all new cellular phones to enable “hands-free” applications.

Because of the high bandwidth requirements of many Bluetooth applications, it is not suitable for low power applications. The greatest energy is consumed in transmission times, and the high bandwidth mandates relatively large packet sizes, implying relatively long transmission duty cycles, even for infrequent operations.

Bluetooth is, however, readily suitable for transmission of audio information, and is now routinely found in headsets for cellular applications with many hours of operation between recharging applications.

3.1.3 ZigBee™

In general, ZigBee was developed as a low bandwidth sensor and control wireless protocol, and can operate over a variety of frequency bands, including the 2.4 GHz Industrial, Scientific and Medical (ISM) bands. Like Bluetooth, ZigBee has both consumer and industrial power levels available with output power ranging from 1mW for short range operation to 50mW with ranges specified as up to one mile.

In the presence of interfering signals, such as wireless phones, Bluetooth devices, or similar consumer devices, every possible mechanism for avoidance of interference has been employed.

First and foremost is handshaking – a valid response from the receiving controlled device indicating that a command was correctly received.

Second, is use of a signal amplitude such that the control signal amplitude is likely to be sufficiently greater than interference signals – effectively capturing the receiver.

Third is a mechanism for selecting an unused frequency for communication. ZigBee Pro introduced this capability in the form of frequency agility – the ability to sniff out unused channels for utilization in interference environments.

As it turns out, this is both an asset and a liability. As a result of the improvements in reliability and ability to operate in a complex environment, ZigBee has now been selected as a replacement for home controls for future applications. Thus the possibility of a crowded environment with resulting increased latency exists. While this may be of no significance when the latency increases for changing a television channel or adjusting volume of an entertainment system; it will likely be unacceptable for critical control features such as control of a mobility device.

In the near term, ZigBee Pro meets virtually all of the requirements for industrial control and even for medical information, including high levels of security and self configuration and even for current applications in control – although no latency tests have been discovered to date. Thus, ZigBee Pro may be acceptable as a design for wheelchair and other assistive living devices if short latencies can be demonstrated.

The comparison of described commercial protocols is listed in Figure 3-1.

Protocol / Features	ANT	ZigBee™	Bluetooth™	Wi-Fi™
Application Focus	Personal Area Networks	Monitoring & Control	Cable Replacement	Web, Email Video
System Resources	3KB	32KB	250KB+	1MB+
Battery Life (days)	200 – 1000+	100+	1-7	0.5 - 5
Network Size	2^32	2^64	7	32
Bandwidth (kb/s)	1000	20 - 250	720	11,000
PCB Area (mm^2)	100	100+	100+	Large
Range (meters)	1 - 30	1 – 100	1 – 10+	1 - 100
Success Factors	Ultra Low Power Power and Ultra Low Cost	Power Cost	Cost, Convenience	Speed Flexibility

Figure 3-1 Comparison chart - protocols.

In summary, ANT is highly recommended for environmental monitoring and healthcare applications. However, its competence of handling critical control functions is doubtful. It is stated that the channel message rate ranges from 0.5 Hz to 200 Hz, but the power efficiency, transmission robustness and system latency are not guaranteed for high data rates. ANT does not support customization of the packet length, which is considered as a shortcoming for power conservation.

In comparison with other commercial protocols, ANT features ultra-low power and ultra-low cost, which are primary success factors for developing a commercial product. Furthermore it offers simplicity in protocol architecture to facilitate the development of the project. Therefore, even though the disadvantages of ANT present, it is still considered as a prominent platform to quickly prototype the infrastructure of wireless networked control on an assistive mobility device and demonstrate it through non-critical applications.

3.2 System Architecture

An existing wired architecture of a power wheelchair is usually composed with major seating and driving blocks, which is shown in Figure 3-2.

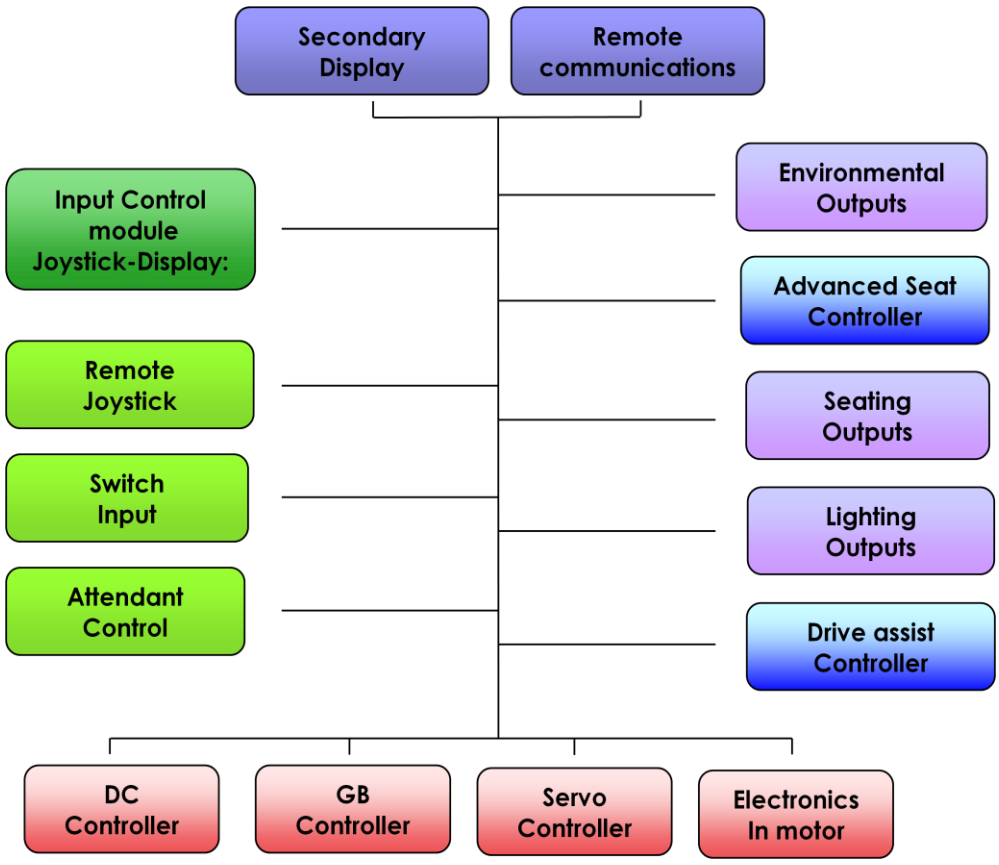


Figure 3-2 Wheelchair control system major blocks.

The architecture gets progressively more complex as new technologies emerge. Future systems will need flexibility to allow new technology to be deployed as required so that solutions can meet both the functional and financial requirements demanded. Wireless communication is an enabling technology for achieving this goal. The major blocks of the wheelchair can be categorized in terms of compatibility of wireless techniques:

1) Wireless techniques are not applicable over devices which are energy-consuming, e.g. servo controller. Since wireless nodes are usually powered by cell battery or energy harvesting, they ideally suits data transmission but not actuator operation.
2) Wireless techniques have difficulties to handle control applications which require very high data transmission rate and signal integrity.

A hybrid wireless network architecture is proposed. Many sensing and functional nodes are transferred from wired to wireless to provide more opportunities to expand systems, while other nodes that require high power and reliability remain wired and form the backbone of the system. This hybrid architecture is illustrated by a block diagram shown in Figure 3-3:

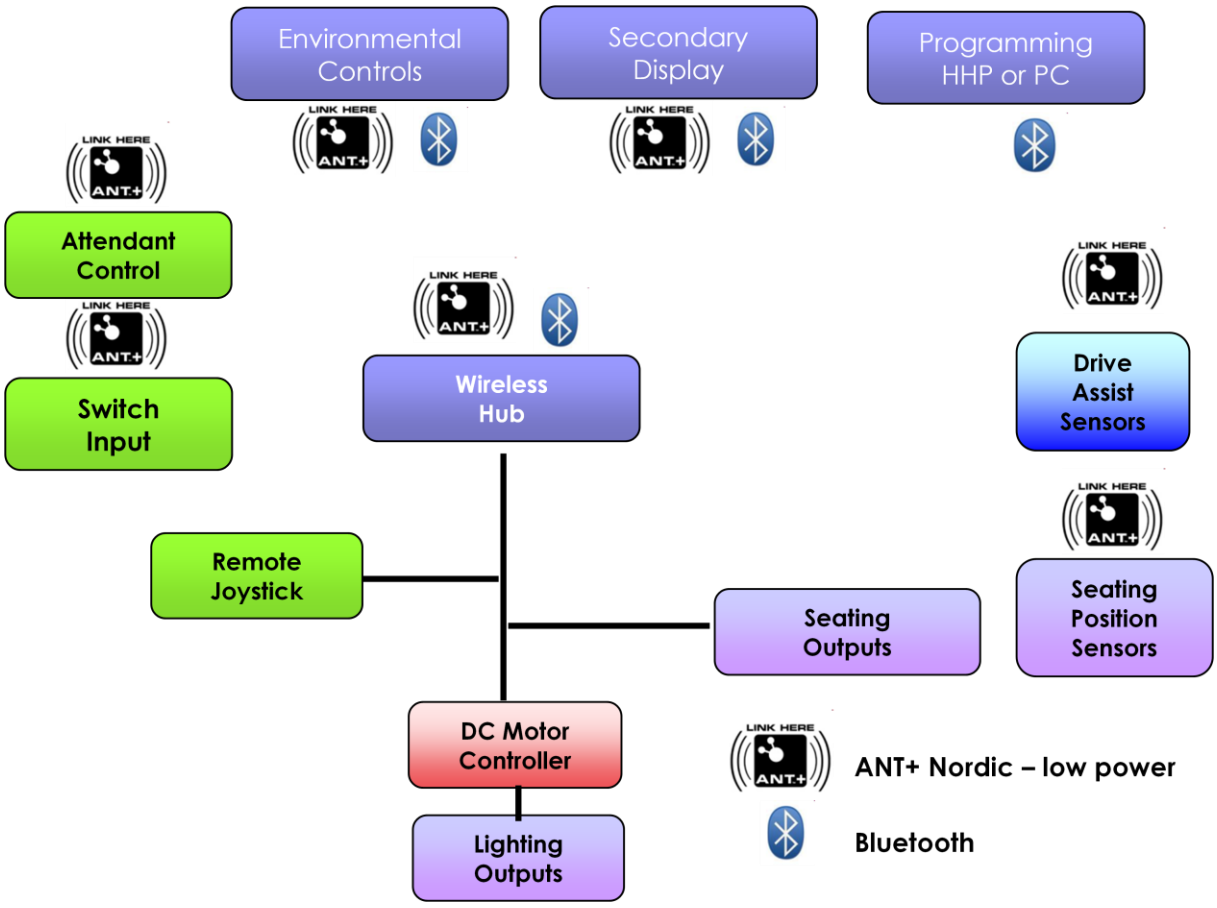


Figure 3-3 A hybrid wireless network architecture block diagram.

As shown in Figure 3-3, wireless technologies offer complementary solutions to the existing wired network. The whole system presents a hybrid architecture. In this hybrid network architecture, we can classify nodes into wireless nodes or remote node (only connected via wireless links), wired nodes (only connected to the wired network) and gateway node or hub node (connected to both wireless and wired network). The wired network is the backbone and powered by a main battery. DC motor controller, lighting outputs, remote joystick and seating outputs are all wired nodes, since they usually drain a large amount of power or perform primary user control. Wired backbone satisfies the requirements for such applications because the main storage battery with large volume of energy supply and its immunity to interference. Drive assist sensors, seating position sensors, attendant control and switch input are wireless nodes, which are power constrained, dedicate to low-rate and low-power applications with limited mobility. A wireless hub is a gateway node, which acts as a) a network gateway to provide access control to the wireless network; b) a network coordinator which constructs and maintains the network; c) a protocol convertor which converts the received wireless information to a format that can be interpreted by the wired backbone. The scattered wireless remote nodes are deployed on the wheelchair to perform various tasks, to enhance the functionalities. They provide two sets of functions: one is to sense the environment, collect data and provide feedback to the system, such as seating position sensor and drive assist sensor; and the other is to provide user interface to achieve remote control, such as remote joystick and attendant control.

In this project, the wired network employs CAN BUS protocol, and the wireless network is based on ANT protocol. Bluetooth may be a complementary solution for system expansion as many commercial Bluetooth products are available in the market. For future perspective, wireless applications will embrace more emerging technologies: environmental control, secondary display and wireless HHP. Some of wireless applications is listed in Table 4:

Position sensors for seating	- Wireless micro-switch for actuators - Wireless tilt switch for seat angle
Wireless attendant control	- Simple wireless proportional joystick control - Advanced wireless control with Joystick, speed-pot, mode switch
Environmental control	- Transferability between beds and wheelchair - Remote control on windows, doors, lights, TV set and etc.
Secondary display	- Run-time information display using other commercial products, e.g. iphone
Wireless HHP	- Remote program or configure the system via wireless links - An option that should be considered, but market evaluation is required

Table 4 Wireless applications table.

3.3 Hardware Design

The platform supports system programming, debug and test on both embedded platform and PC interface. The block diagram of the prototype platform is shown in Figure 3-4.

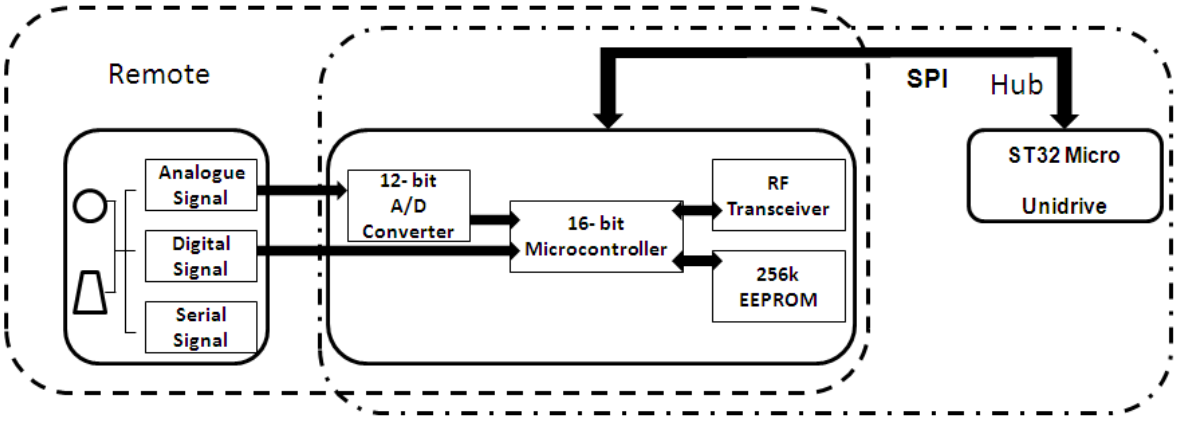


Figure 3-4 Platform Structure.

This architecture will be applied on both master and slave nodes for prototyping. The features of the platform include:

- Supports two SPI channels for interface with both transceiver unit and serial input.
- External memory for ID management.
- JTAG for both run-time debugging and PC interface.

The overall design of the complete platform consists of five functional blocks and three interfaces. The five functional blocks include RF transceiver unit, protocol driver (the 16-bit microcontroller), digital input, analogue input and external memory. Three interfaces consist of a Joint Test Action Group (JTAG) interface and two Serial Port Interfaces (SPIs). JTAG interface is used for programming and debugging purpose on Microcontroller Unit (MCU). One of the SPI channels is designed for driving the RF transceiver and the other one is used for communications between the wireless prototype and wired backbone of the power wheelchair through Unidrive. The schematic design for both complete platform and cut-down platform are shown in Appendix A.

The RF transceiver unit

The COTS RF technology employed in this project is ANT+. ANT+ is the enhancements based on the ANT core stack enhanced with several new features. An interface for drop-in module is preferred rather than designing the circuitry of ANT+ transceiver. The selected ANT+ core drop-in module is ANTAP281M5IB with connector interface rather than surface mount. The

connector selected is Molex 52991-0208-C as recommended on data sheet of Development Kit [1].

The serial interface to the host MCU can be either synchronous or asynchronous depending on the configuration of the pin-outs and both interfaces are supplied in PCB design. Status and data messages are transferred bi-directionally to create and maintain communication channels, transmit data to and receive data from peripheral sensors and devices [2]. The interfaces for ANT+ transceiver is shown in Figure 3-5.

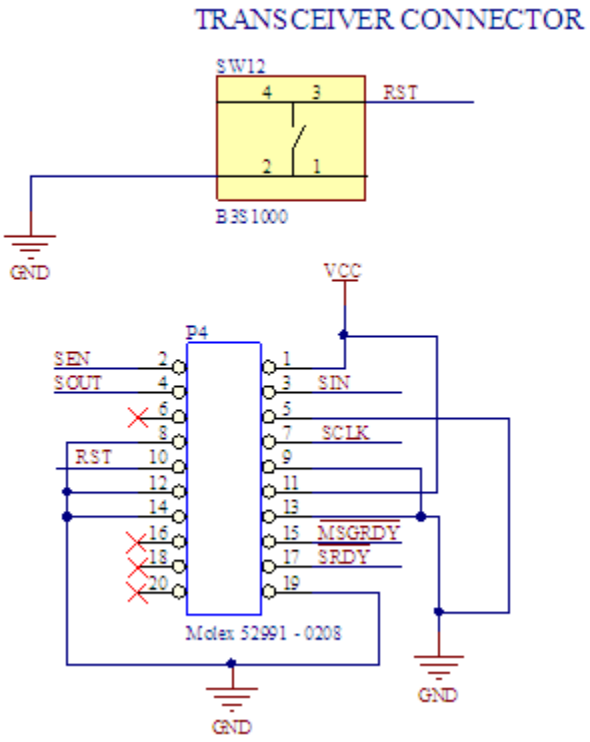


Figure 3-5 Transceiver connector.

Protocol Driver

The microcontroller in use is a MSP430F2410, with 56KB+256B flash memory. The MCU will be embedded with the ANT/ANT+ protocol. It provides the analogue and digital inputs and outputs, four serial interfaces and two I2C channels.

The reason to select MSP430 chipset is due to its ultra-low power feature, and ease-to-implement. It is the standard component employed on the AT3 chipsets which are parts of the General Purpose ANT Chipset family, thus it is easy to kick-start the project with reference design provided with Development Kit.

The on-board microcontroller can be programmed and debugged using JTAG interface. A PC interface will be developed via JTAG as well for testing and data collecting for prototype performance [3].

For ultra low power applications, the MCU contains one 16 MHz high frequency oscillator and one 32.786 KHz low frequency oscillator. The low frequency clock can also be synthesized from the 16 MHz crystal oscillator clock. This saves the cost of a crystal but increases average power consumption because a significant power will be consumed for clock synthesis. In this project, a 32.786 KHz oscillator is employed.

Two SPI channels are designed; one for the transceiver interface, the other SPI channel is used for serial communications with the commercial products in Dynamic Controls Ltd.

Power Supply

Two power connectors and one voltage regulator are used on the main board to provide a steady 2.5V supply. A coil cell battery holder is designed for remote applications due to its light weight and small size. However, for most of the development time, the prototype will be programmed and debugged via JTAG interface. Thus, a DC power jack will be suitable for supplying power under this circumstance to conserve the energy of coin cell battery.

The Vcc range for EEPROM 24LC256 is 2.5-5.5V, for ANT transceiver is 1.9 -3.6 V and is 1.8 – 3.6V for microcontroller. Thus a 2.5V power supply will satisfy the requirements from all the IC components. The voltage regulator is adjustable, so that the supplied voltage of 2.5V can be increased to 3V if 2.5V is too low to support stable performance for EEPROM.

On-board Input Devices

The input devices contain ten switches and three potentiometers to provide digital and analogue inputs respectively. The analogue input ports are connected to internal 12-bit Analog-to-Digital (A/D) converters built in the host microcontroller. Two headers provide interface with external digital/analogue input devices such as temperature sensors, accelerometers and etc., which extends the applications of the platform.

A scenario with mixed input signals from different devices will be developed on the prototype board. Therefore signals from different devices can share the message packets to optimize the transmission efficiency. This will be extremely useful when the RF solution is transferred to a power wheelchair system, so that the modules are able to share the message packets if they are in close proximity and allowed to be deployed on the same PCB board.

3.4 Summary

This section presents some work packages prior to system developments, including protocol selection, overview of existing power wheelchair system and hardware design of wireless prototype.

ANT protocol has been selected to build a wireless platform for wireless applications on a power wheelchair, which offers ultra low power and low cost RF solution for commercial products. It is a light-weighted wireless protocol with only 1 KB protocol stack for protocol driver, minimizing the cost on host MCU. The transmission range of ANT protocol is up to 30 meters, which is sufficient for applications on a power wheelchair.

The power wheelchair system is built based upon CAN BUS backbone, so that the wireless platform is required to interface with the existing system architecture. The wireless solution aims to provide complementary functionalities rather than replacing the existing wired system. This requires a hybrid architecture which consists of both wired and wireless devices. In this section, we also envision the application domains of wireless solution on a power wheelchair, which help define the requirements of wireless platform development.

The hardware design of the prototype is intended for testing and demonstration purpose of the wireless solutions. To avoid burden in designing the RF transceiver and antenna, we decide to employ a drop-in module solution provided by ANT. The schematic and PCB layout are shown in Appendix B and Appendix C respectively.

Chapter 4 ID MANAGEMENT

In a wireless control network, a node usually represents a sensor module, an actuator or a control input unit within a mobile system. For the purpose of network construction and maintenance, an ID management module is required for the network coordinator to recognize, register and manage the device nodes in the network. ID management needs to manage the RF nodes by using attribute-based identifying and location –based addressing.

In this project, we aim to design an ID management module with intelligence to achieve autonomous network construction and maintenance.

This chapter is organized into three sections: Section 1 describes different methodologies for device pairing. Section 2 presents device localization methodologies which are essential for the network coordinator to obtain the physical topology information where each device node is installed. In Section 3, we establish an integrated ID management system to perform network self-organization through demonstrating a case study.

4.1 Device Pairing

Device pairing enables two nodes to establish a reliable wireless connection. In this chapter, we first present the state of the art in device pairing, and describe the requirements of device pairing in this project.

Extensive research works have been undertaken in device pairing. Many of them focus on building a secure link for temporary applications [9]. For example, two devices, such as a headset and a cell phone as shown in Figure 4-1, are controlled by a single user. Another example involves two users communicate with each other with a pair of cell phones, as shown in Figure 4-2. In both cases, a priority for device pairing is link security between two devices as the users do not want their data to be publicly available to all wireless devices in range, such device pairing schemes are termed as “Secure First Connect”. However, in this project, device pairing aims to establish permanent wireless links between network coordinator and device nodes to exchange sensing information and user command messages, data security is not a priority in this development. In such a pairing scheme, approaches with high intelligence and ease-of-implementation are preferred.

Figure 4-1 One-user-two-device pairing.

Figure 4-2 Two-user-two-device pairing.

A widely deployed approach is Bluetooth pairing which involves searching a list of devices in range and selecting a target from them with additional authentication procedure using Personal Identification Number (PIN) codes. This is also referred as PIN method. Push Button Configuration (PBC) method is an alternative solution for the users to push a hardware or software buttons on both devices to establish a wireless link. Near Filed Communication (NFC) method allows two devices to connect with each other in near field. A plethora of alternative approaches have been demonstrated, some focus on simplicity [10, 11, 12], and others on security [13, 14, 15]. These different approaches fall into two categories: (1) based on out-of-band (OOB) channels, and (2) based on proximity [16]. These two categories are classified in terms of how the users trigger the device to initialize the pairing process. OOB takes advantages of the use of auxiliary channels, which are both perceivable and manageable by the users who operate the devices [16]. Kobsa, et al. [9] compared devices pairing schemes based on OOB channels. Device pairing based on proximity is to pair devices when they are brought within a close distance with each other [16]. The NFC method described is a proximity-based method. This method usually involves distance detection by using acoustic or Received Signal Strength (RSS) strength.

4.1.1 Device Pairing Strategy for Applications on Power Wheelchairs

This project aims to build a network which performs sensing and control over a mobility system. We begin strategy design for device pairing by looking into the key characteristics of wireless control network over a mobility system:

Data Security: Wireless links are relatively easy to eavesdrop upon or be manipulated. Thus, it is important to secure the links to protect privacy or prevent the links from outsider attack.

However, for a wireless control network over a mobility system, information transmission across wireless links is either environment sensing data or user control command data rather than confidential information, data security is not a major concern in this case.

Robustness: System robustness is a major issue especially for an assistive system which targets for disabilities. The control network needs to maintain and analyze logs of system and network behavior, detect and identify any abnormal activities, ensuring that the system may recover itself as long as any faults arise or otherwise take emergent actions to protect users. Thus, device pairing is expected to offer advantages for the control network in terms of self-recovery and ease of maintenance and repair.

Ease of Implementation: In an ideal setting, device pairing can be accomplished by a naïve user quickly, extemporaneously without explicit instructions. Suppose a wireless sensor node is engaged into the network, how can the network coordinator identify and register the sensor with right configurations (e.g. the position of the sensor deployed and the functionality of the sensor performs)? Search-and-Select scheme through a user interface such as a screen or a keypad on the end devices is a possible solution. However, it is laborious for users and not cost effective therefore it is not a proper solution in this project.

Cost: The target of this project is to develop a networking protocol which can be applied on commercial products. Thus, constraints of cost need to be taken into account. Two criteria need to be satisfied in the design: 1) minimize burden imposed on manufacturing process; 2) avoid the use of auxiliary channels as they rely on either sensors – such as cameras, microphones or accelerometers – or peripherals, such as display or keyboards.

Under these constraints, a strategy for device pairing targeting for a wireless control network over a mobility system has been formulated. It is described as follows:

Authentication is not a major concern for device pairing in this case, this is unlike Bluetooth-enabled devices which usually store and transfer private data. For data transmission across a wireless network of a power wheelchair, security refers to creating a private communication zone to isolate the data transmission from public RF environment rather than protecting data from eavesdropping or outsider attacks.

The scope of device pairing in this case is to construct a star network by associating each end node with a network coordinator rather than the bootstrapping of secure channels between two devices. Thus, the objective is to find a device pairing solution which offers simple, reliable and fast process for network construction and maintenance.

4.1.2 Methodologies for Device Pairing

Device pairing refers a sequence of events through which participants of a channel establish connections between them. The participants need to be aware of special features of each other prior to starting pairing progress to distinguish those participants from others. Such features can be a shared secret, estimation of proximity and etc.

For commercial purpose, we need a device pairing scheme which is applicable for industry products. Based on the analysis in the previous section, we need such a scheme to provide compatibility and mass production of RF devices, which calls for standardization. In principle, standardization in manufacturing process is an effective cost reduction strategy and offers greater flexibility for users. This way user can replace any faulty device with a standard back-up device readily. This means, ideally, all the RF devices are expected to be manufactured with a standard set of hardware design and loaded with a standard set of target codes. However, in such a scheme, device pairing could be very complex because duplicates of RF devices are present. A network coordinator is not able to distinguish each node due to the lack of identities when multiple nodes join into the same network. Thus, more efforts are required to identify each participant node by - for example - through human interventions. To resolve this problem, we need an approach to identify each individual node prior to pairing device. This is achieved by pre-configuring each individual node.

Configurations of a device node include parameters which describe its identity, functionality, priority and etc. These parameters offer all necessary information required to construct, operate and maintain a network, which are illustrated in Figure 4-3. Configurations offer a full description of individual nodes, and the level of descriptions involves a tradeoff between flexibility and ease-of-operation. A device node with only low-level configurations offers great flexibility in terms of capability to perform different tasks together with different wireless nodes, whilst, more efforts required to initialize such a node prior to pairing.

As shown in Figure 4-3, an identifier is globally unique number which provides a primary identity for any other device to recognize it. Device type is a field used to denote the type (or class) of each participating network device, and provides information to decode message. The global unique identifier and device type are categorized to be node-specific fields. The configurations in these fields are considered to be global identity for an individual node. Network number is a shared secret for restricting nodes to join into a private network. The network only grants access to a node only if the Network Number at both ends match, providing a measure of security and access control. Local address is a locally unique identifier assigned to a node within a private network. Local topology addresses the position of a device node installed. The network number, local address and topological address fields are

categorized to be network-specific because they are only required while constructing a network, configurations in these fields can be temporary. Functional parameters include all the parameters related to the operations such as search timeout, RF frequency, transmission power, message rate and etc. These fields are protocol dependent and discussed in details in case study. Two arrows indicates that it will be easier to construct a network if more fields of participant nodes have been configured prior to the device pairing, at the price of degrading the flexibility of the nodes. This is because with fewer fields preconfigured, more fields can be configured dynamically according the system requirements during the device pairing procedure, enabling the nodes to be deployed with larger flexibility.

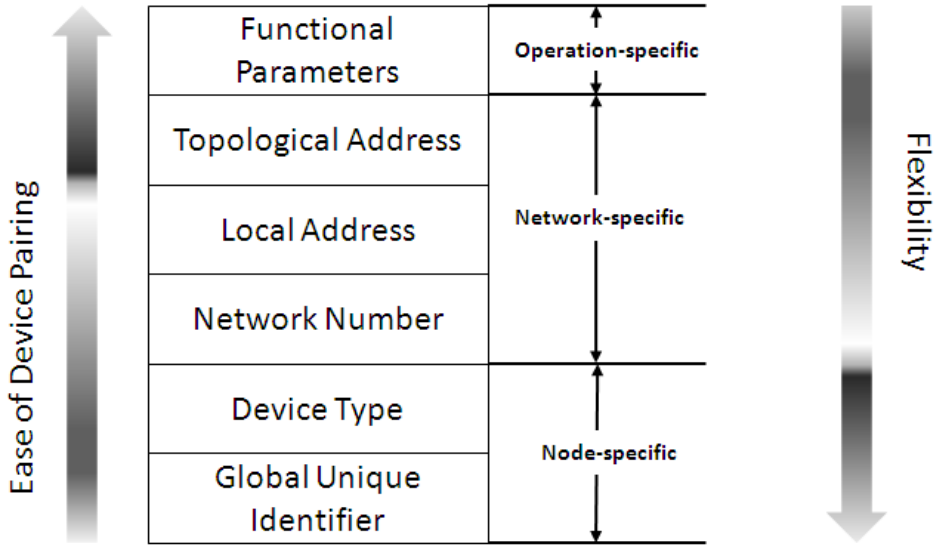


Figure 4-3 Wireless node configuration fields.

The concept of preconfiguration is to those parameters into a node during the manufacturing process. However, for mass production, preloading high-level operation-specific parameters such as message rate, RF frequency and search timeout is time-consuming and laborious. Furthermore, it degrades the flexibility of device pairing in the sense that RF devices are deprived of the capability of automatically reconfigure themselves to work with different types of sensors and control units. In contrast, low-level device-specific such as unique identifier and device type, preconfiguration retains flexibility of devices and can be executed automatically in manufacturing line. For device pairing, a unique identity field is the baseline for network construction. However, for network-specific parameters such as Network Number, there are different strategies to deal with it.

With networking-relevant configuration field fully defined, network construction is executable with different device pairing schemes:

1. For each individual mobility system, preconfigure all the nodes which are intended to be deployed onto this system with a common shared secret (e.g. network key) before device pairing procedure initialized. This is referred as the standard paring protocol.

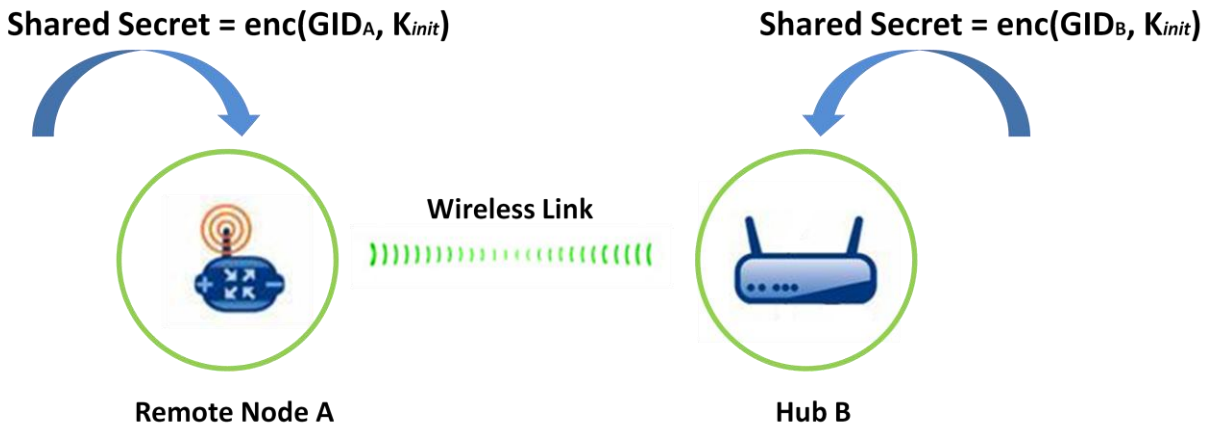


Figure 4-4 Standard pairing protocol.

As shown in Figure 4-4, a link key K_{init} is already loaded into a pair of wireless devices, A and B, prior to device pairing. The link key value is encoded with global unique identifiers GID_A and GID_B on both devices. The standard pairing enables two devices to pair with each other by a handshaking protocol to mutually authenticate each other.

2. Only one device stores a shared secret on each mobility system, and all the other devices "read it" using auxiliary channels. Many recent works proposed different pairing methods based on this strategy, such as "Seeing-is-Believing" method [18].

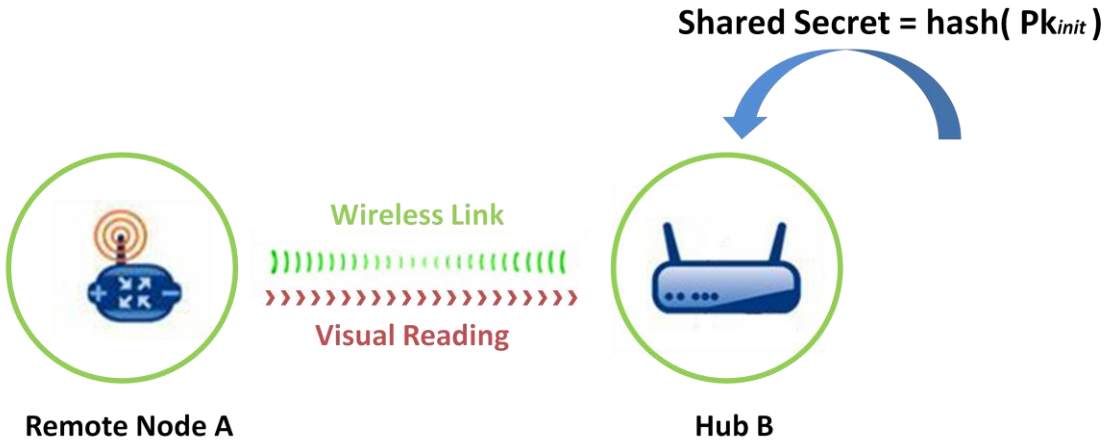


Figure 4-5 Seeing-is-Believing pairing protocol.

As shown in Figure 4-5, in this scheme, PK_{init} is a public key and it may be either permanent or ephemeral depending on the protocols. It can be encoded by two-

dimensional barcodes or images, the other devices read the key through visual channels (e.g. camera). Seeing-is-Believing is a simple solution to implement device pairing by reading the shared secret, but camera is required at least one end, which is not practical on sensor motes. However, this strategy is fascinating for simplifying the device pairing protocol as one hub with pre- authenticated key is able to pair with other nodes without any specific configurations.

3. Both devices for pairing establish a secret value by manual verification, and generate a secure link key. This methodology relies on human authentication for initializing device pairing. Most Bluetooth-enabled devices employ such a scheme [19].

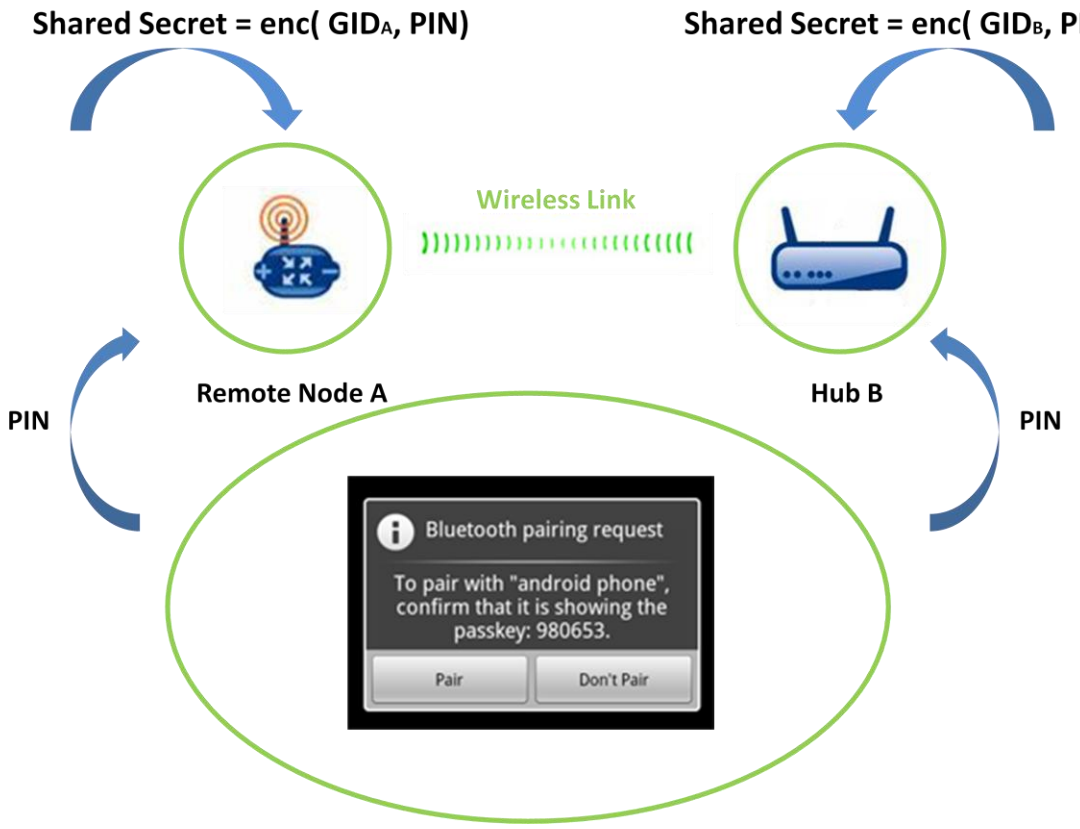


Figure 4-6 Bluetooth pairing protocol.

In Figure 4-6, a standard pairing scheme for Bluetooth is shown. The association procedure between two devices, A and B, is initialized by sharing a low-entropy, human-memorable secret value *PIN*. Both devices have access to each other's global unique identifiers GID_A and GID_B. Initially, one device searches all other Bluetooth devices in a range, and the user selects one of them on the searching list to request an access, the device receives the request message will inform that a pin value is required. The

handshaking protocol starts once a pin is confirmed. This scheme provides secure channel link, but human intervention is imposed on the pairing procedure.

4. Devices associate automatically when they are brought within a close distance of each other based on proximity estimation [20]. For many commercial RF platform products, proximity detection has already been an embedded module, which offers opportunities for applying proximity-based device pairing on commercial products.

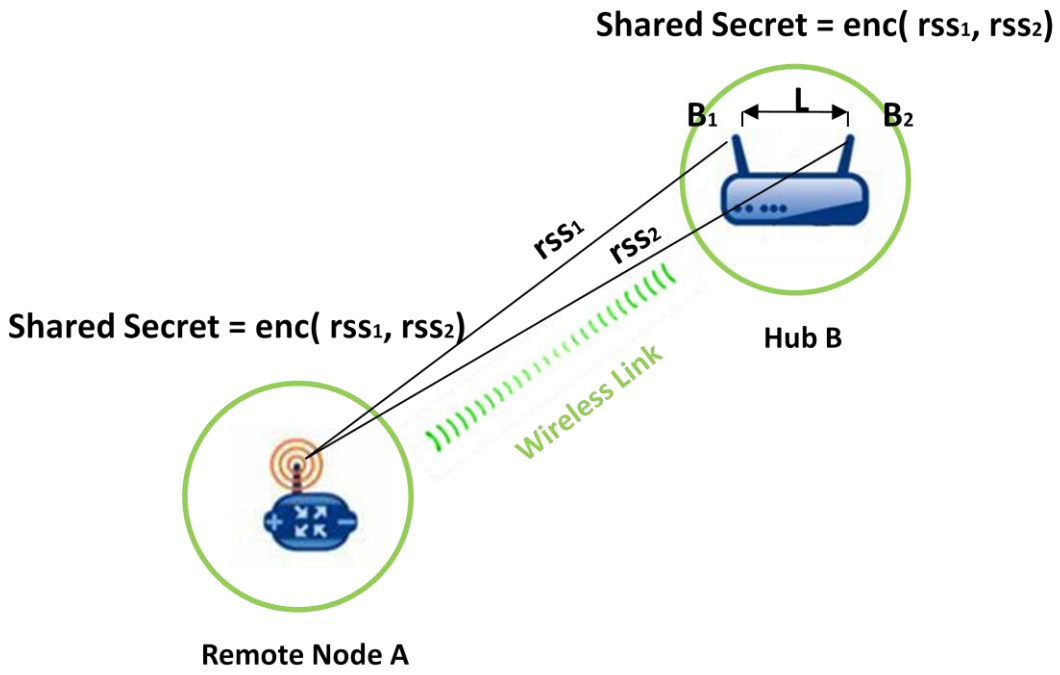


Figure 4-7 Good neighbor pairing protocol.

In Figure 4-7, a pairing scheme based on proximity detection is illustrated. This is referred as Good Neighbor pairing scheme which is described in [20]. In this scheme, the receiver has two antennas B_1, B_2, separated by a distance L. While a message is received at hub B, distance is estimated by measuring the RSS rss_1 and rss_2 on each antenna respectively. These RSS measurements generate a shared secret on both ends for device pairing.

4.1.3 Usability Studies on Device Pairing Methodologies

Although many device pairing methods have been proposed by current research works, each one has certain advantages and shortcomings. Therefore, a comprehensive and comparative usability study needs to be conducted prior to identifying the most suitable solution for this project. We overview the listed device pairing methods, perform analyses to evaluate these paring methods in terms of usability (e.g. ease of use, cost and pairing speed) and reliability (e.g.

error tolerance, system diagnosis and recovery). Many research works comparing different pairing schemes [21], [22], have focused on device pairing for peer-to-peer wireless communications, e.g. a single user controls two devices and two devices each controlled by its respective user, the contribution of this project is to conduct a comprehensive and comparative field study, focusing on device pairing for wireless network construction.

The requirements of device pairing in such a scenario can be derived from characteristics of wireless control network over a mobility system which has been described. These include: cost, ease of use, robustness and data security. In addition, for commercial purpose, we need to minimize the potential burden imposed by device pairing on both the manufacturing process and the end users.

Preconfiguration of shared secret offers advantages in terms of simplicity for end users and security for system. All the RF nodes which are intended to join a network have been pre-loaded with a common shared secret before installation, a network coordinator broadcasts informing messages to all the nodes with the same network key and then registers them into the network automatically. This approach requires least amount of human involvements and offers security feature as well, as the shared secret has been encoded and encrypted in the RF device and prevents device pairing procedure from eavesdropping.

The challenge of this method arises due to the difficulties that users may encounter if they need to add a new RF device into the system. For instance, a user may have to replace faulty devices with new ones. In such a situation, the user needs to perform preconfigurations with explicit instructions and PC operations to load network secret of the intended network into the new nodes. As a consequence, this technique is highly constrained by the capability of users and availability of PC tools. From perspective of supporting facilities, an interface port (e.g. a serial port) for communications between RF devices and PC must be integrated on the device, and a support software tool is required to perform preconfiguration. As such, this approach is neither user-friendly nor cost-effective. Hence, it is not applicable for this project.

Reading a shared secret from other device is usually implemented in an OOB channel for data security. OOB channels are both perceivable and manageable by the users. Thus, the transmission across OOB channels is controllable by the operators to authenticate information exchanged over wireless channels. OOB channels rely on either sensors or peripherals to exchange information in a dedicated channel or a separate band to distinguish pairing information from normal operation data. This approach has certain flexibility. For each mobility system, one node (e.g. network coordinator) carries a shared secret, and all other nodes read it and reconfigure themselves automatically. This enables a network coordinator to pair with any other node which has not been assigned with a specific shared secret. However, auxiliary

devices are involved in such a scheme, resulting in higher cost. Moreover, this scheme usually relies on manual intervention for pairing procedure.

Pairing by manual verification (e.g. a low-entropy PIN value) is a proper approach to establish a transient link between two devices. During the pairing process, the two devices involved establish a wireless link by creating a shared secret (usually a user-input PIN code). The advantage is that the shared secret is encrypted prior to pairing, protecting data transmission from eavesdropping. The link can be deleted from either end. A peripheral device (e.g. keypad) is required for human interventions.

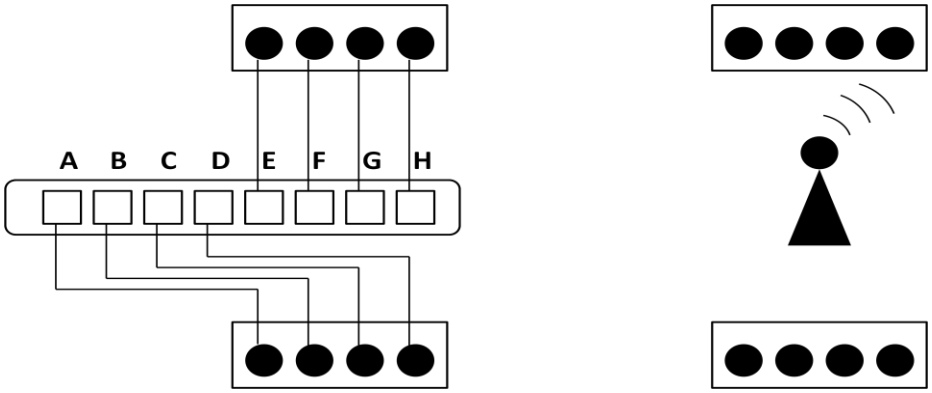
Device pairing may use proximity estimation instead of a shared secret. In this scenario, the RSS is measured at the antennas for retrieving relative distance between two devices based on a Log-normal shadowing model [23]. Device pairing based on proximity estimation offers enhanced functionality, a network coordinator is able to localize a node while pairing. This is a very useful feature especially if functionalities of wireless nodes are associated with the position they are deployed. Many current commercial wireless products (e.g. ANT+ core nRF24AP2) offer proximity estimation module, which makes proximity-based device pairing applicable for commercial products. However, applications of this methodology are still quite limited. To take advantages of antenna diversity, multiple antennas are expected to be built in a wireless device and spaced, this will make the receiver board large and expensive. The resolution of proximity estimation based on RSS measurements is limited. In consequence, this pairing method may misidentify multiple nodes which are placed in a confined space. Besides the RSS measurement is highly environment-dependent: uncertainties may be caused by scattering, RF interference and etc., especially in a dynamic environment. Thus, this method is not practical for device pairing of a wireless control network over a mobility system.

Device pairing by either reading a shared secret from other device or manual verification is a possible approach for constructing a wireless network over a mobility system. However, manual verification approach relies on peripheral devices for user input, which is laborious and increases hardware cost.

In the application dealt by research work, it is proposed that reading a shared secret can be carried out without need of any auxiliary devices in this scenario. This is because data security is not a prominent consideration in this a scenario, we can remove the use of auxiliary channels. One device can read a shared secret from other device through a normal operation channel rather than a dedicated channel, the shared secret is transmitted in a public RF environment. Thus, this method does not provide Man-In-The-Middle (MITM) protection. However, the device pairing procedure is entirely autonomous, no user interaction being involved.

4.2 Device Localization

Device localization is a primary task for the system to realize effective ID management. This will require extrinsic operations on the system to obtain location information of device nodes. An intelligent device localization solution needs to be developed to facilitate managing and maintaining the control network on a mobility system. These solutions of device localization are modularized as a Location Discovery Module (LDM) and interact with network protocols via an interface with autonomy to reduce the amount of manual effort required to carry out this task.



(a) Wired Infrastructure (b) Wireless System

Figure 4-8 A ultra-sonic sensing parking system.

Location discovery refers to the problem of coordinating scattered remote nodes deployed on different locations. The functionality of a node is associated with the location where the node is deployed. As shown in Figure 4-8, eight distance sensors (A - H) are integrated into the frontier and rear bumper of a vehicle. The system needs location information of each sensor to aggregate the collected data. For wired infrastructure, the system is able to locate sensors by the physical connections between sensors and ports (Figure 4-8 (a)). However, this is not the case in a wireless network (Figure 4-8 (b)): system requires the location information prior to registering the nodes which are installed into the system.

In recent years, there has been increasing amount of research effort devoted to localization problem in wireless domain. Most node localization solutions are developed for several domains covering military surveillance, environmental monitoring, and habitat monitoring and structural monitoring. In these applications, node localization aims to accurately find the location of each node in a large scale wireless network system. The objective of node localization in such schemes is to offer advantages for motion tracking [24], [25], [26], [27], [13], [28] in a dynamic environment or improve network functionality in terms of routing [1]-[3], bandwidth and path length optimization [4]-[6], power management [8] and security [7].

However, device localization within an automotive system aims to provide information of node position for identifying functionalities of a node. In the remaining part of this section, we will establish the need for device localization within a mobility system and conclude the design strategy from analysis of the need. Furthermore, we will present different techniques that enable localization and meet the requirements.

4.2.1 Need of Device Localization

This thesis deals with node localization of a wireless control network over a mobility system. While deploying a large number of wireless sensory devices around a mobility system to perform comprehensive detection and monitoring tasks, a network coordinator requires the spatial knowledge for processing data received from wireless nodes. For example, a power wheelchair is equipped with multiple distance sensor nodes, it is crucial for the network to identify the physical coordinates of each node to determine the orientation of distance measured from each sensor. In such a scenario, localization refers to relative position rather than absolute geographic position. This is a critical consideration for sensor identification, data fusion and data analysis in many applications [33], [34]. Device localization, in such a scenario is also termed as physical topology discovery, has attracted extensive research has been conducted recently [29], [30], [31], [32]. Within a self-constructed wireless network, topology discovery is a prerequisite to many applications.

The applications of device localization are divided into three categories based on their functionalities.

Device deployment and installation: With self-localization schemes, a large number of wireless devices can be deployed and installed over a mobility system quickly. The network coordinator will obtain topology table with autonomous.

Network diagnoses and maintenance: For a wireless network to work reliably and robustly, it is vital to quickly and accurately detect and diagnose the faulty nodes. In such a process, topology discovery plays an important role.

Energy conservation: With known physical topology of each individual node, network coordinator manages the node activities dependent on the mobility system activity in real time. For example, while a wheelchair is driven forward, distance sensors equipped in rear may enter idle mode for conserving power.

4.2.2 Methodologies for device localization

The design strategy of localization methodology is application-specific. In this thesis, localization aims to aid in constructing, operating and maintaining the wireless control network on a power wheelchair, this can be characterized as follows:

1. **Static framework**: A network is classified as static in the sense that most nodes are stationary once a desired topology is formed, a few nodes (e.g. remote user control unit) may move around with limited mobility. Topology discovery is only processed during the construction stage of the network.

2. **Multi-functional network**: For a WSN in which all the nodes perform one particular task (e.g. position tracking, temperature sensing), physical topology is the only attribute for node identification. However, wireless control network is an operational, multi-functional network with a mixture of different sensors and user input units to collaboratively perform comprehensive environment and system monitoring and control. Thus, in such a case, node identification is based on both sensor type and topological location.

3. **Spatial limitation**. Within an automotive system, a number of nodes are deployed in a confined space, thus it becomes difficult to obtain location information by calculations based on distance and angle measurements due to the constraints of resolution of existing technology. The physical structure of an automotive device results in a scattering-rich environment, hence the measurements are prone to errors due to multi-path fading and scattering.

4. **Network topology**. This wireless control network employs a wireless infrastructure mode with star or tree network topology, which means that a set of end nodes connects to a central unit (coordinator or router) directly. The control network can benefit from centralization with ease of deployment, ease of upgrades and so on. However, the localization algorithm is not able to take advantage of multi-hop information, i.e. obtaining location information from estimation of other nodes.

5. **Hardware requirement**. To keep the overall network economically feasible, additional hardware aims for localization (e.g. directional antenna) should be avoided whenever possible. This keeps the size of the nodes small as well. Thus, it is preferred to use existing capacities which are available from commercial RF products (e.g. RSS measurements).

6. **Practicability and flexibility for end-users**. One of the objectives of this project is to develop the wireless control network to facilitate mobility systems which are user-oriented. From this point of view, the device localization methodology needs to offer ease of use and robustness for end-users. On the other hand, it is essential to investigate on

different localization techniques so that the LDM allows a range of access control to provide diversity and redundancy.

The main contribution of this section is to create wireless node localization solution which is oriented to the wireless control network applications over a mobility system (e.g. wheelchair, automotive and robot). This is different from localization systems and algorithms aim to create universal applicable solutions in outdoor or indoor environments. The aforementioned requirements pose significant challenges. One such challenge is how to achieve fast and accurate topology discovery with power-efficiency and low cost.

Physical topology discovery can be based on 1) topology table (TT) or 2) radiolocation technique (RT). Topology table is predefined in the network coordinator, which stores topology-relevant information. Topology table maps distinctive characteristics (e.g. a unique identification) to topological locations. In a wireless environment, such identification is required to be encoded into an RF message frame and delivered to the network coordinator. Topology discovery based on topology table is fast and reliable. However, this approach relies on the predefined topology table and predefined triggering events: while a new node not listed in the table is joining into the network, operational burden will be imposed for reconstructing topology table and triggering events.

Radiolocation technique relies on sophisticated hardware which is capable of obtaining different physical variables for either distance measurements or triangulation. The Global Position System (GPS) is a well known example which relies on the time difference of the arrival (TDOA). Other physical variables include: received signal strength indication (RSSI), angle of arrival (AOA) and time of arrival (TOA). Radiolocation technique can be applied for both global geometric localization and local topology discovery. Many previous studies have been conducted on the network topology discovery, e.g. Criket [35], DV-Position [36], AHLoS [37] and SeRLoc [38]. These different localization schemes aim to different application domains, according to the requirements (e.g. measurements, accuracy) and constraints (e.g. hardware cost and size, power consumption, operation environment).

4.2.3 Triggering Mechanisms for Topology Retrieving

In this thesis, data aggregation is not our prominent consideration as we propose to build an infrastructure for wireless control networking over a mobility system which has only a limited number of wireless sensors and control units, particularly for demonstration purpose. To simplify the project, we assume that the physical topology information of all the nodes have

been predefined in a topology table. Data aggregation in this project is discussed in this section only for future perspective. Thus we will focus on the different approaches which can be used in conjunction with topology table, while a study on radiolocation techniques is beyond the scope of the thesis due to the resource constraints.

For a wireless control network, the redefined topology table can be tracked by different approaches:

1. Pre-configure the remote nodes and store the physical topology information in the firmware of the nodes. This approach simplifies the device pairing process. However, it reduces the flexibility of the remote nodes: a pre-configured node can be only deployed onto a particular position which has been defined. Otherwise it has to be re-configured prior to deploying it anywhere else.

2. Associate each remote functional node with a unique pattern of socket which has been defined in the topology table in the hub node, as shown in Figure 4-9. Device pairing through the socket pattern is realized by a socket mounted on the system, two headers are reserved for power line, and the other headers are used for generating unique pattern to identify the position of the node, e.g. ON state responds to “1” and OFF state to “0”. While a wireless device node is plugged into the socket, it reads the power state of each header and encodes it into a message frame to broadcast to the network coordinator. The message carries the topology information of this node which is unique in the network, corresponding to its unique location within a system. This solution facilitates the pairing process of the remote nodes by reducing the effort of manual operations. However, a socket is required, this may be impractical for the remote nodes which are required to be installed in the locations where a socket cannot be placed, or a socket may render the design some potential disadvantages.

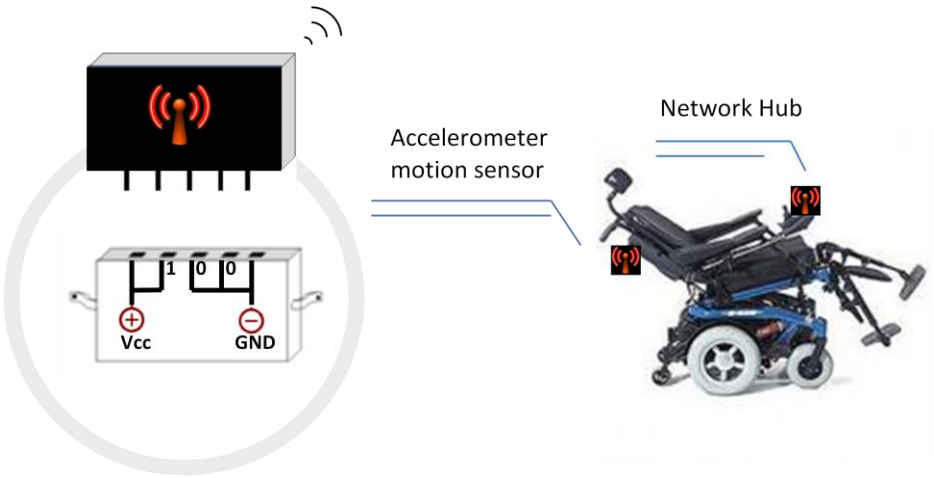


Figure 4-9 Logic pattern triggering.

3. Identify the position of a node by generating actions as shown in Figure 4-10. In some locations, it is possible to recognize a remote node by manipulating the system. For example, a 3-axis wireless accelerometer is mounted on a leg rest position of a wheelchair to sense the motion of it. While the leg rest of the wheelchair is lifting, accelerometer can capture the movement and feedback to the network coordinator. Thus, the network coordinator can identify its physical topology by linking it to the topology table, according to the feedback message received from the wireless node. This approach takes advantages from the hybrid structure of the control network, while a wired node (e.g. a leg rest) is already defined in the system topology table, a wireless node can be localized by linking its collected sensory data to some particular action of a wired node. This provides a complementary solution when the remote sensor nodes are designed to be installed in the places where a socket does not fit.

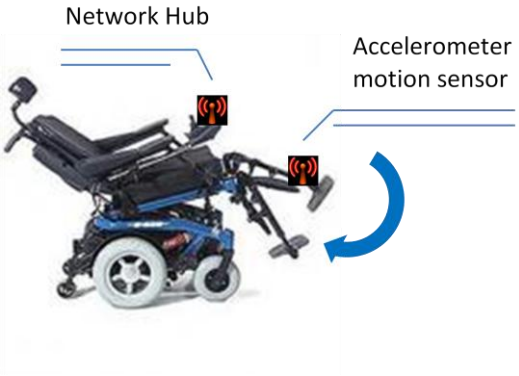


Figure 4-10 Action detection triggering.

4. A user interface is provided for users to visually control the process of a remote node to access the network through manual operations. A graphic user interface (GUI) can be developed for locating the devices by a user interventions. The predefine topology table is visually illustrated on a screen and offers access control for users. Each time while a new node is engaged into the network, the device pairing procedure is activated after users have indicated the physical topology of the node through GUI operations. The GUI can be a software package which is implemented on PC platform, and interface with a mobility system via cables (serial port or USB) or Bluetooth link. This solution fits all the devices without any limitation for localizing any wireless device node. However, the GUI software needs to be updated to obtain information of up-to-date devices information while advanced new modules which are not included in old version GUI intend to be employed.

These different methodologies allow remote devices to be engaged into a system network with different accesses, and provide users and industry program with a range of controls over the system. This design also builds redundancy into the network architecture to achieve high-degree of reliability. These four approaches offer multi-layer architecture of device pairing process. During the device pairing, they are invoked in a sequence according to their priorities. To organize the layered architecture, it is essential to characterize these approaches and determine the priorities of each one.

4.3 Implementation of Device Pairing on a Power Wheelchair with ANT+ Core Wireless Platform

ANT protocol offers a pairing mechanism base on channel configurations. Each channel is established between, as a minimum, a single master and a single slave participant. One master node can support a large number of slave nodes. The master acts as the primary transmitter and the slave as the primary receiver. Messages are always transmitted from the master node to the slave node at the designated channel period (Tch). It is optional that slave node sends back a message back or not in the reverse direction. This is shown in Figure 4-11:

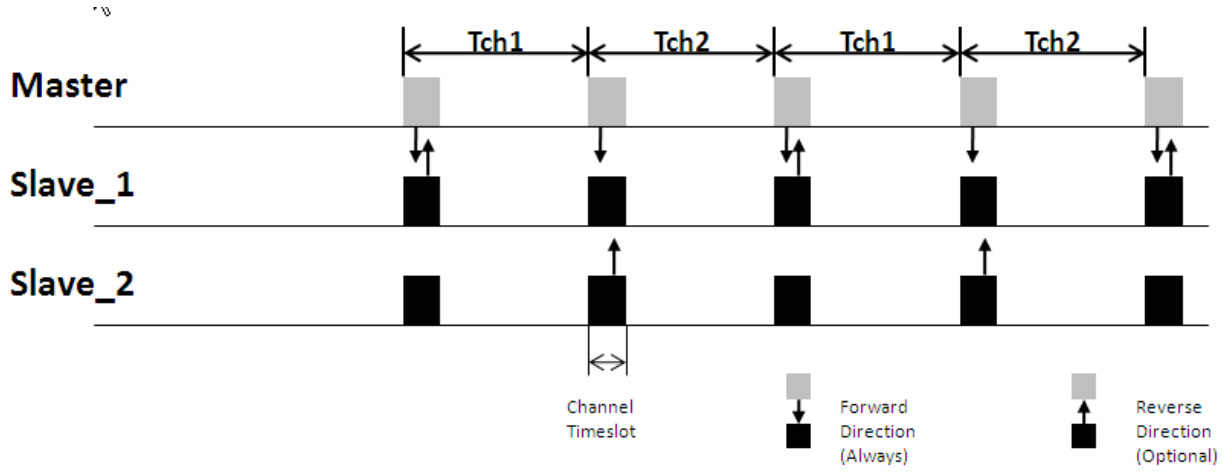


Figure 4-11 Channel communication.

In order to establish a communication link between two ANT nodes, they require a common channel configuration that includes operating-relevant information. The details can be reviewed in [39].

Channel ID is the crucial field to device pairing: only two nodes with matching Channel ID can establish a wireless link. Each wheelchair can be assigned with a common Channel ID, all the wireless nodes mounted on this wheelchair hold this Channel ID and constructs a private network. The private network, in this context, is not defined to secure access to intended participating devices, as Network Key does. Instead, it creates a protected RF environment for filtering data message from ANT devices from other networks in the proximity. Channel ID is a 4-byte filed that contains 3 fields – Transmission Type, Device Type and Device Number. These three fields can be user defined, and the channel between two nodes can be established based on the predefined infrastructure scheme as shown in Figure 4-12. This is a standard procedure provided in ANT. More details can be found in [94].

In this pairing scheme, configuration fields of both nodes have been fully defined for establishing a peer-to-peer communication link. Note that the configuration fields within the dashed line box have default settings and require setting only if a new parameters are desired. The other fields, however, have to be defined with certain values. Network Number and Network Key work together to provide an encrypted access for secure device pairing, a particular Network Number has a corresponding Network Key, and only channels with identical valid Network Key are able to communicate with each other. If an invalid Network Key is assigned, it will be recognized as default Public key automatically. Private Network Key costs up to $5950.00 US per key to obtain the license. Only the public Network Key is free for development but it does not provide the encrypted access. In this project, the field of Channel ID is defined as a common secret for establishing a private wireless channel. Channel ID is used to narrow down the selected device to associate and pair with. On a single device, multiple channels can be assigned with the same Network Number and Network Key. However, Channel ID must be associated to a particular channel. In order to establish a channel, the master node must specify

its Channel ID and the slave node must hold the Channel ID it wishes to search for. Only the Channel ID at both ends match, the channel can be established between the master node and the slave node.

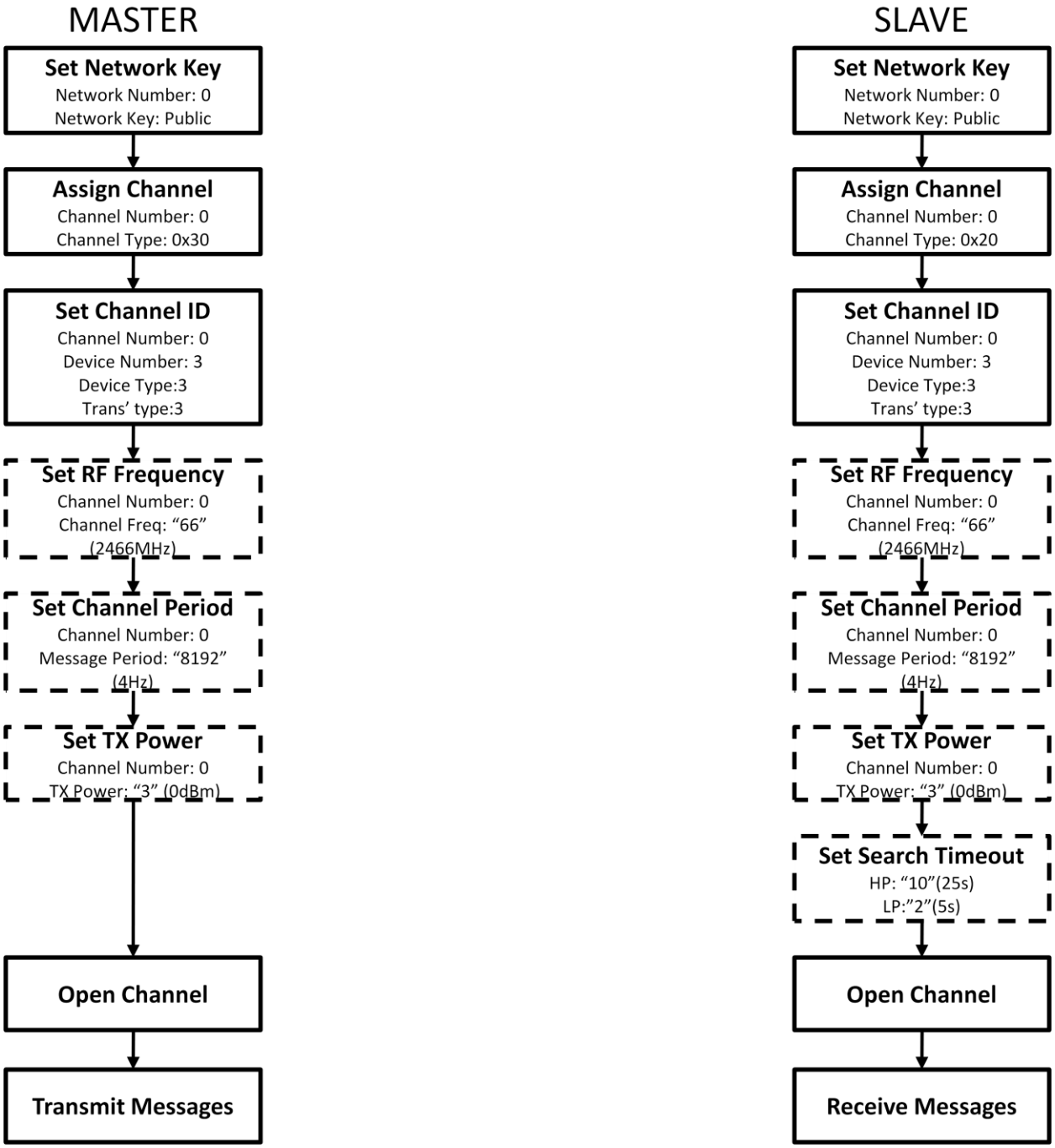


Figure 4-12 Process to establish communication channel [39].

We propose to develop a network topology with a base station mode. In this topology, a gateway node (master) corresponds to register and coordinate all remote nodes (slave), and the remote nodes are able to be added into or removed from the network with ease and

flexibility. The network topology is denoted as auto shared network, which is shown in Figure 4-13.

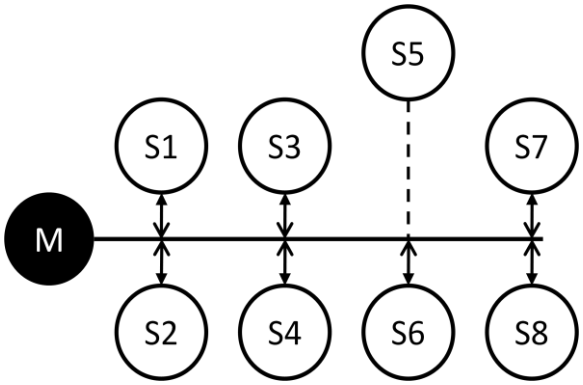


Figure 4-13 Auto shared network.

To achieve this goal, we propose an auto paring scheme. This pairing scheme consists of two phases: 1) a gateway node registers a remote device node into the network with a unique local address; 2) the remote device node is assigned with a private Network ID.

A private network can utilize Channel ID field. Within each network, the gateway node stores a unique Channel ID, and each participant node reads it from the gateway node. However, the local address field is not associated with any default configuration field, and we need to define it by using data payloads. The serial message for communication between host MCU and ANT transceiver is defined by ANT protocol, and the basic format which is shown in Figure 4-14:

Sync	**Msg Length**	**Msg ID**	**Channel Number**	**Data_0**	**Data_1**	**…**	**Data_N-1**	**Check sum**

Figure 4-14 ANT serial message structure.

Table 5 describes each component of the serial message:

Byte #	Name	Length	Description
0	SYNC	1 Byte	Fixed value of 10100100 (Write flag) or 10100101 (Read flag), the LSB indicates the direction of communication
1	Msg Length	1 Byte	Number of data bytes in the message. The number of bytes following the Msg ID with Checksum byte excluded.
2	MSG ID	1 Byte	Data type identifier, indicating the functionality of this message. Details can be found in [40]
3	Channel Number	1 Byte	The particular channel which this message is assigned to, this information is not included for the messages which are not relevant to a particular channel
4…N+3	DATA_1…DATA_N	N Bytes	Data bytes
N+4	CHECKSUM	1 Byte	XOR of all previous bytes including the SYNC byte for error checking

Table 5 ANT message description [39]

This is the basic format for various serial messages, including configuration messages, control messages, notification messages, data messages event/response messages and etc. The details is presented in [41].For data messages, broadcast, acknowledged or burst, the data payload is fixed with 8 bytes. We can reserve one- or two- byte field as local address field to specify the source or destination of a data message.

Data_0	Data_1	Data_2	Data_3	Data_4	Data_5	Data_6	Data_7

Channel Data Payload for Peer-to-Peer Communication

Local Address LSB	Local Address MSB	Data_0	Data_1	Data_2	Data_3	Data_4	Data_6

Channel Data Payload for shared channel Communication

Figure 4-15 Message payload format

The ANT shared channel suits wireless control network where a centre node receives data from a large number of wireless remote devices. The number of slave nodes supported is determined by the number of shared address bytes. Theoretically, with 2-byte addressing, more than 65k slave nodes can share a single master node. The shared channel communication scheme provides ease for network nodes management to avoid the problem of channel contention among multiple slave devices. This also enables the polling of each individual slave nodes to retrieve the received data, enhancing the reliability of network scheduling. The channel operation flow is shown in Figure 4-16.

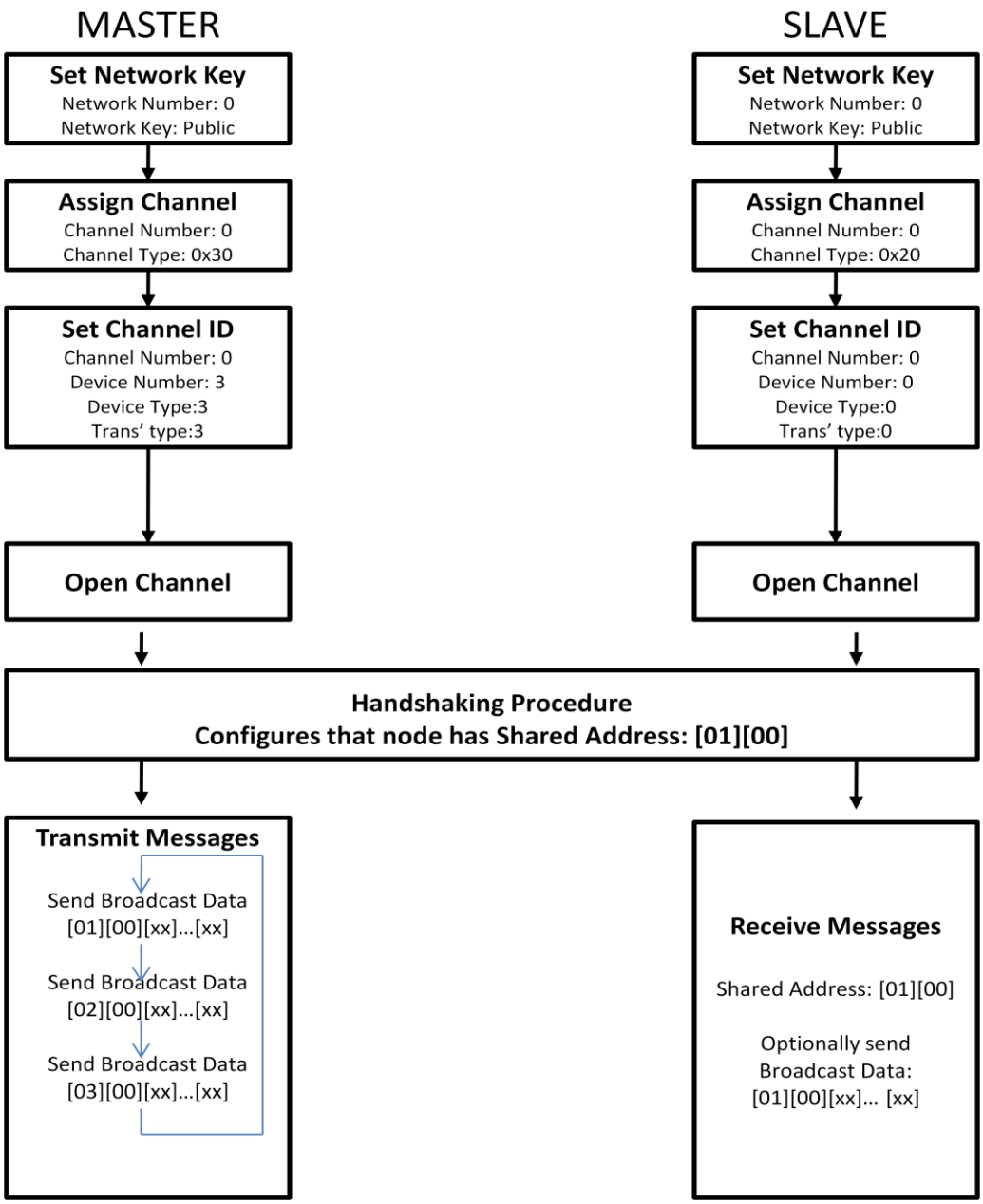


Figure 4-16 Shared Channel establishment and operation.

In Figure 4-16, the shared channel is established based on an assumption that the master node needs to pair with a slave node without a shared address assigned. This scheme allows master node to pair with an arbitrary number of slave nodes with unknown address and the slave node to be registered into and removed from the network dynamically. This requires an auto-pairing procedure for a master node to control and manage the multiple slave nodes. The auto-pairing functionality is encapsulated into simple Application Layer state machines together with a handshaking procedure.

It also shows that the Channel ID of the slave node in Figure 4-16 is set to zero, which is a public Channel ID that enables the slave node to be associated with master nodes with different Channel IDs. This auto-pairing procedure will also enables the slave node to be merged into a private network by resetting its Channel ID from public to private scheme.

This auto-pairing handshaking procedure begins with a set of initial conditions which is essential for device pairing:

1. A master node is identified by a unique 4-byte Network ID;
2. Every slave node has a unique 4-byte manufacturing serial number.

A master node employs 8-channel chipset for capacity, and the channel 0 is dedicated to auto-pairing for ease of management. The auto-pairing procedure is confined to channel 0 on both master and slave nodes. This converts the unique manufacturing serial number into a local shared address, constructing a private network.

The pairing procedure is triggered by pressing a button in a safe zone, and then the master node will enter into pairing mode for registering a new node. If there is more than one master node in close proximity to each other, they must not be triggered into pairing mode simultaneously so that they will not register a slave node which is not intended.

State machines are used in both master and slaved device to ensure that the pairing procedure is managed with a step-by-step approach. The state machines will only progress into the next stage if certain criteria are met. These criteria can be either a particular received data message or a channel event/response message. We will overview the essential stages required for auto-pairing first and then define the criteria for each stage.

The auto-pairing starts by broadcasting a message to inform that there is local address available (Address Available Message) in the master. The slave receives it and request to acquire the local address by sending back a Request Address Message which also contains its unique serial number. Since the Address Available Message is a broadcast message and may be received by many slave devices, in order to avoid contention between multiple slaves, the master sends a broadcast message (Busy Acquiring Message) with the received serial number to inform that the local address has been assigned to that particular slave. The serial number is a globally unique 4-byte field assigned to each slave node. The slave node receives it and confirms the local address being assigned by sending a Confirm Acquire Message. This is illustrated in Figure 4-17.

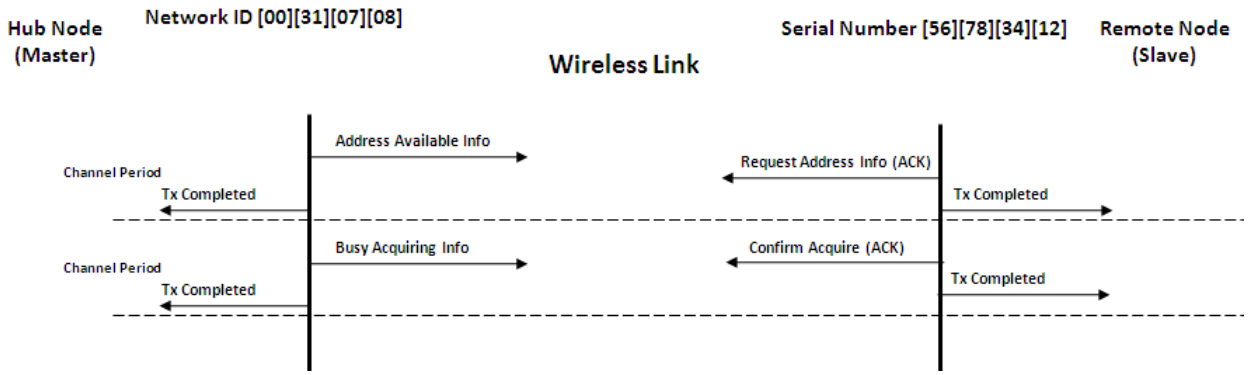


Figure 4-17 Simple handshaking procedure.

During each channel period, a serial of command messages are sent back and forth between the master and the slave nodes. The slave nodes always send an acknowledged message back to the master to ensure that it will only progress onto the next stage if the message is received and acknowledged by the master.

Assume that the first two bytes of data message payload is reserved for local addressing, the third byte is specified to carry command (CMD) information. The message format for each handshaking message is listed in Table 6:

Source	Command	Type	Shared address	CMD	DATA_1	DATA_2	DATA_3	DATA_4	DATA_5
Master	**Address Available**	**Broadcast**	**[FF][FF]**	**FF**	**00**	**00**	**Data Timeout**	**Available Local Address**	
Slave	**Request Address**	**Ack**	**[FF][FF]**	**FD**		**Unique Serial Number of Slave**			
Master	**Busy Acquiring**	**Broadcast**	**[FF][FF]**	**FE**		**Unique Serial Number of Slave**			
Slave	**Confirm Acquire**	**Ack**	**[FF][FF]**	**FC**		**Unique Serial Number of Slave**			
Master	**Address Full**	**Broadcast**	**[FF][FF]**	**FB**					
Master/ Slave	**Normal Data**		**Assigned Local Address**						

Table 6 RF handshaking messages [42].

In the example shown in Figure 4-18, a master node informs that local address 0x0001 is available by broadcasting an Address Available Message (0xFF), and a data timeout value 4 (8s) is suggested in the case that the device pairing procedure retries while it is not completed within that period. The shared address is specified to 0xFFFF during the entire device auto-pairing procedure so that the device nodes are able to distinguish the pairing command messages from normal data messages. Thus, this shared address is reserved for device pairing only. While the message has been broadcast, a channel event message Event_Tx is sent from ANT transceiver to notify the host MCU that a broadcast message has been transmitted successfully. Note that during each channel period, a message will be transmitted automatically,

if no new message is desired, the previous message will be automatically transmitted. In the sequence diagram below, the messages in dashed line are the automatic messages but not relevant to the auto pairing handshaking procedure.

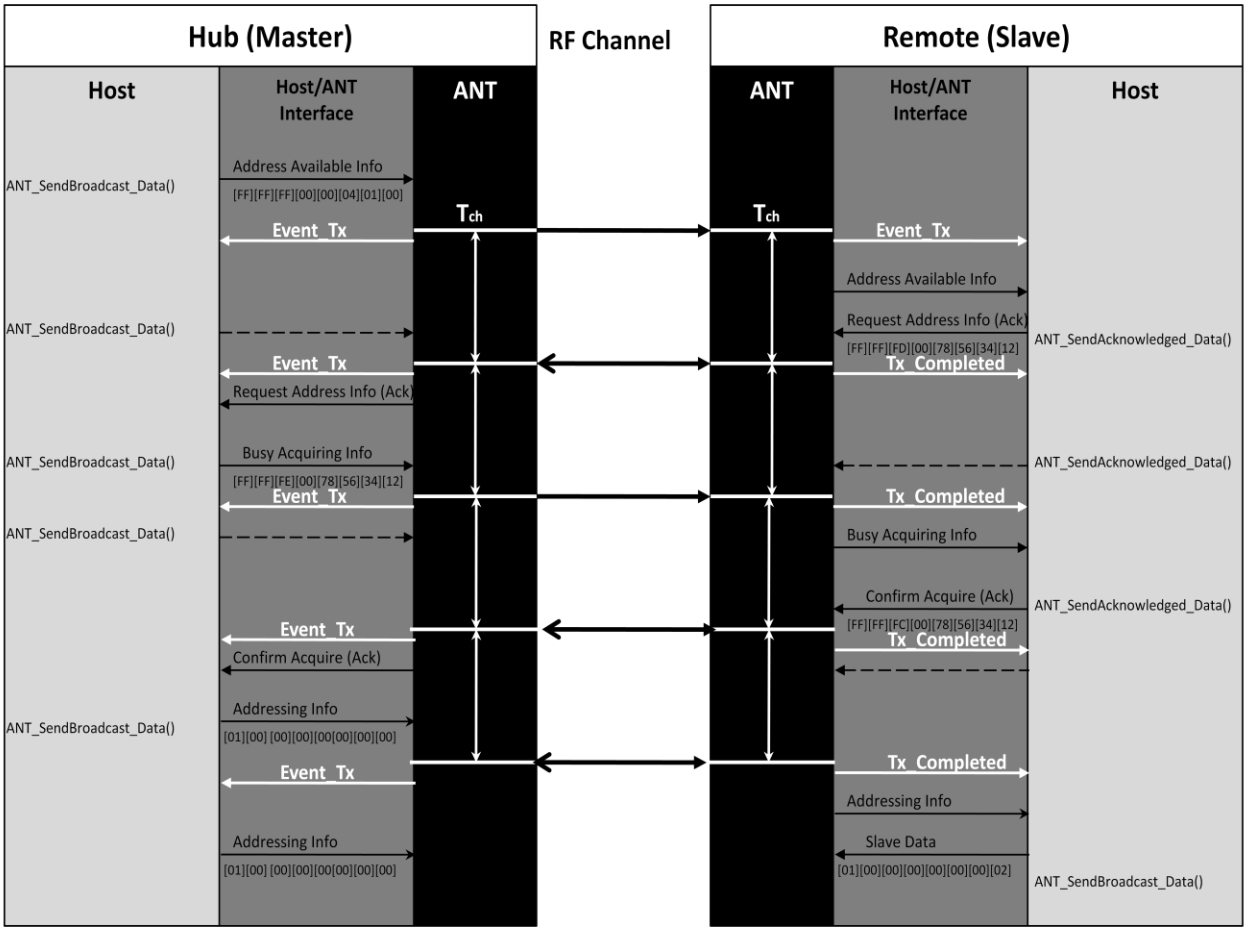


Figure 4-18 Auto device pairing sequence diagram.

Any slave node receives the Address Available Message will send back an acknowledged Request Address Message (0xFD) which contains a 4-byte unique serial number to the master. In this example, the serial number is 0x12345678. A channel event message Tx_Completed is generated by the ANT transceiver to notify the host MCU that the acknowledged message has been successfully transmitted and the automatic receipt has been confirmed.

The master transmits a Busy Acquiring Message once upon receiving the Request Address Message from the slave. Within this stage, the master acquires the unique serial number of the slave and records it for identifying the particular slave to which the local address is assigned to. The Busy Acquiring Message contains the acquired unique serial number, therefore it is broadcasted to all network nodes, but only one slave recognizes it.

At this point, only one slave with the matched unique serial number will continue the pairing process. The slave will send back an acknowledged Confirm Acquiring Message. While the

automatic acknowledged receipt is confirmed by the slave, the auto pairing procedure has been completed.

Then, both the master and the slave start normal operations, a master send a polling message to each registered slave node. If the slave has data in the buffer, the data will be sent in the reverse direction during the next timeslot. Otherwise, the slave has option not to take any action. In the Figure 4-18, the slave sends a data message which is 0x02.

The state machine shown in Figure 4-19 encapsulates the different stages that the pairing process will go through, and the conditions for progressing them.

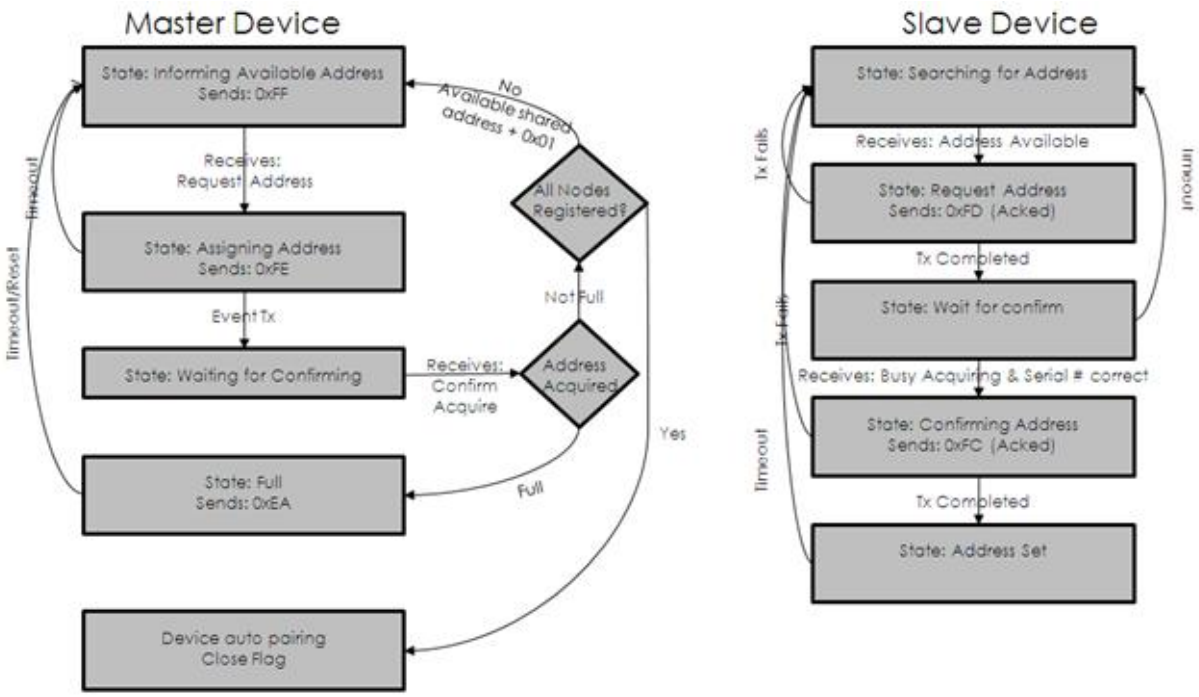


Figure 4-19 State machines for auto-pairing.

For multiple remote devices to be engaged into the network, the master node will repeat the auto device pairing procedure until either an end flag is raised to indicate that all the remote devices have been registered into the network or state is full which indicates that all the available shared address have been assigned to the remote devices.

The auto device pairing scheme allows a wireless node to be added onto and removed from a network dynamically. Any user is able to replace the faulty component on the runtime without instructions or training.

However, although the slave is assigned with a unique local address, the master does not have knowledge about the functionality and position of the slave, the registration process has not been completed.

In Figure 4-20, a back position sensor is installed onto a power wheelchair. The transceiver block (with embedded RF transceiver module, sensor module and on-board battery) is plugged into a socket and activates the circuitry by on-board battery. A particular ON/OFF sequence is generated, and this sequence is predefined and recognizable by the system. The host MCU reads it and forwards it to the ANT transceiver. The ANT transceiver reports it to the wireless hub by sending a RF message, enabling the wireless hub determine the functionality and position of the node by scanning a lookup table.

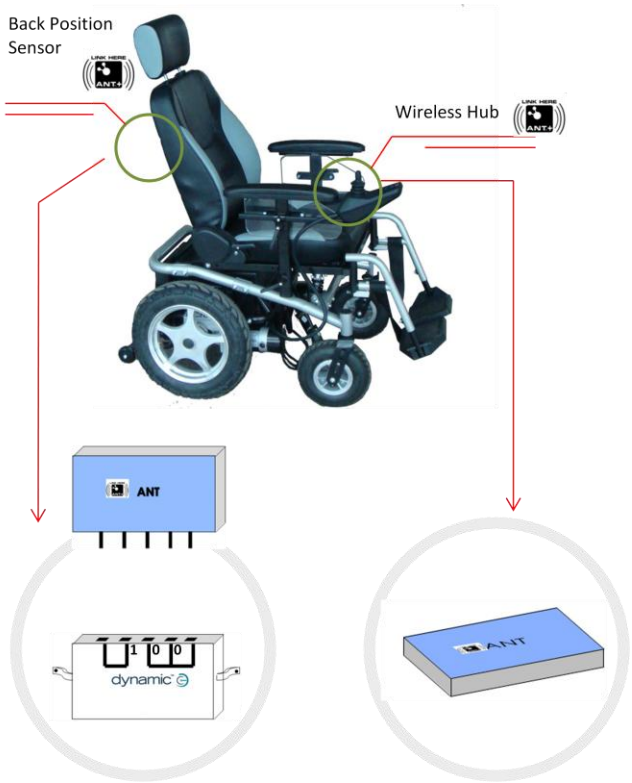


Figure 4-20 Installation of wireless node.

The wireless hub then registers the node into a log-in table, and the registration process has been completed. The log-in table will register all the information of the node for reestablishing the link while it is lost or reset. The basic format of the log-in table is shown in Figure 4-21.

The parameter fields in the log-in table are categorized into two different types according to their characteristics: 1) static parameters; 2) dynamic parameters. The shared address, device type, priority and location parameters are static and used for decoding and processing the messages. Other parameters like operation mode and power mode will change according to the status of the power wheelchair. These fields need to be updated during each channel period according to the system status and determine the corresponding actions.

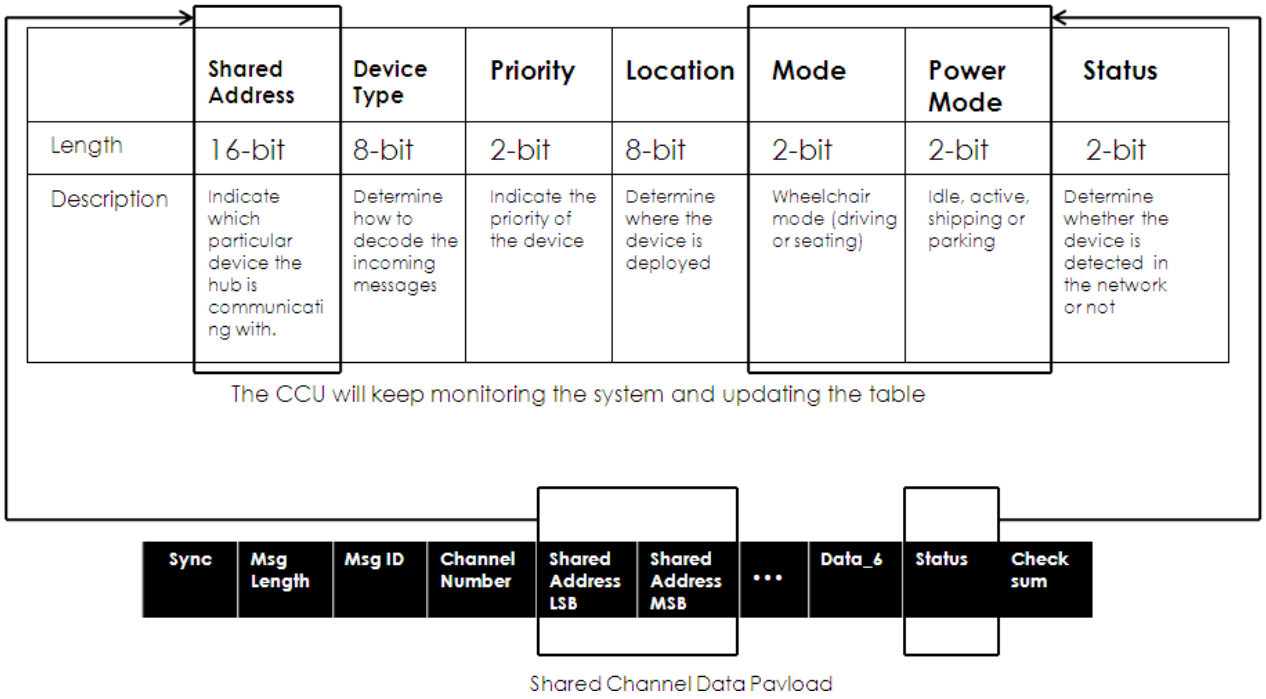


Figure 4-21 Log-in table format.

However, at this point, the Channel ID of the slave remains public. This may cause potential confusion while multiple wireless hubs are present within its transmission range. The slave node needs acquire the Channel ID of the master and reboot itself from the public network into the private one. This scheme can be applied only if the requirements for security are not strict. Otherwise, a high-level security development will be required.

Prior to normal operation, the dedicated channel for device pairing, channel 0 will be closed at the master node and channel 1 will be opened for data transmission. Correspondingly, the slave node will switch from channel 0 to channel 1 to trigger the normal operation. This approach offers ease for channel management, as the each channel can be preconfigured with different requirements for different operations (e.g. device pairing, data transmission and etc.), and the node only needs to switch between different channels to perform different tasks.

The flow chart for node installation is shown in Figure 4-22.

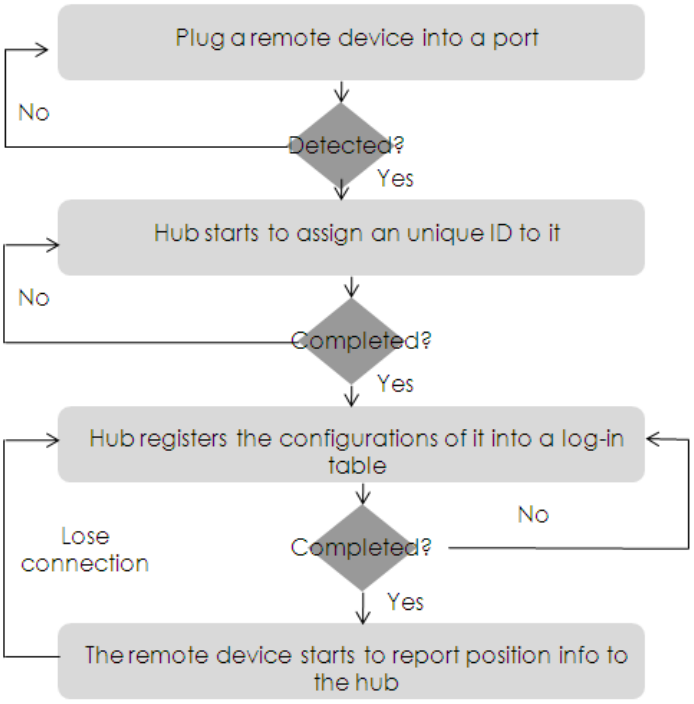


Figure 4-22 Device pairing flow chart.

Therefore, the entire device pairing process can be illustrated in Figure 4-23.

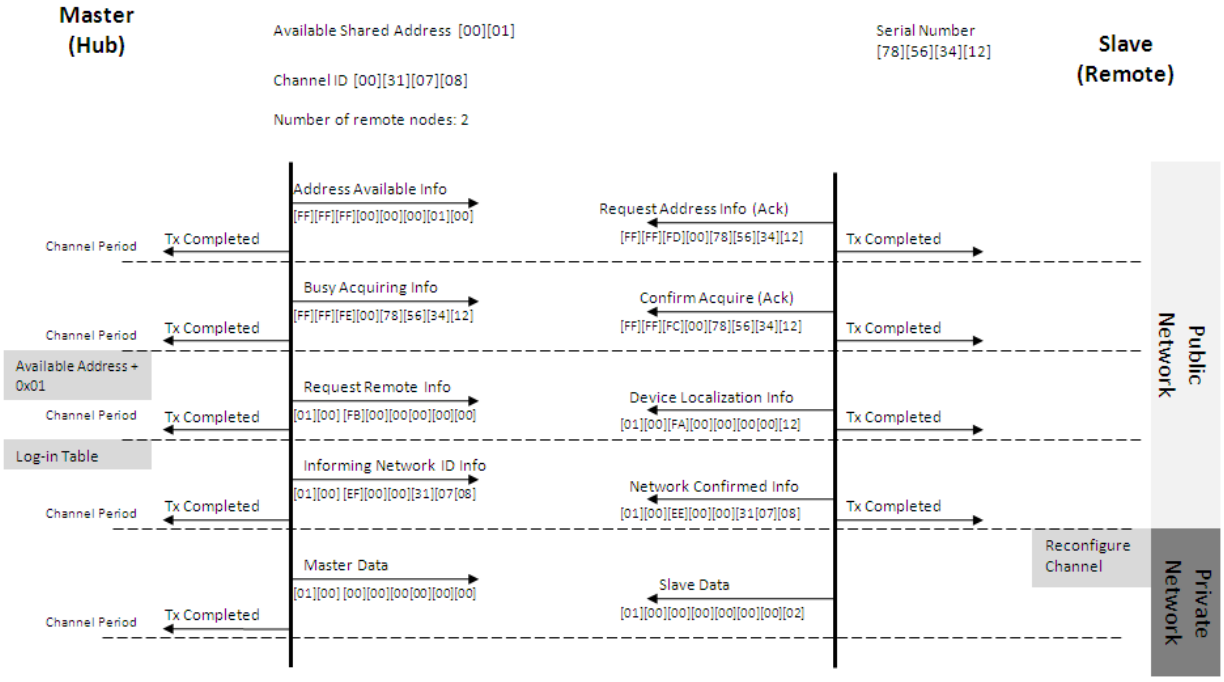


Figure 4-23 Auto pairing handshaking procedure.

Figure 4-23 shows that the auto pairing is composed of three stages. In the first stage, the hub node assigns an available shared address to a remote node, and the available shared address value increases by 0x0001. This stage ends with the reception of a Confirm Acquire Message at the master end. During the second stage, the remote node reads the socket pattern as shown in Figure 4-20, the unique socket pattern within a network indicates the physical topology of the device. The remote node thus encodes it into a Device Localization Info Message to transfer it to the master node while a Request Remote Info Message has been received. Then the master node records the physical topology information of the remote node into a Log-in table for interpreting data message received from it for system operations. The third stage begins with sending an Informing Network ID Message from the master to the remote node, and it informs the network ID of the network to the remote node as a shared secret to restrict the wireless communication between two nodes within a private network in order to avoid cross platform communication between multiple wheelchairs. The remote node will reconfigure its channel ID while it receives Network_Confirmed_Info message to build a private wireless link with the hub node.

Three stages are implemented during the auto device pairing stages. The first stage is operated in a public network environment so that the hub node is able to communicate with any remote nodes which intend to participate into the network. In the second stage, the hub node reads physical topology of each participating node and completes registration of the node. During the final stage, the remote node reads the common secret (the Channel ID of the hub node) and reconfigures its Channel ID to construct a private network. To successfully accomplish the auto device pairing procedure, the hub node needs to be initialized with an available shared channel address as a starting point, the maximum number of participating remote nodes and a unique 4-byte channel ID. The slave node must be configured with a unique 4-byte manufacturing serial number to differ it from any other nodes.

4.4 Summary

In this chapter, we have developed an ID management method which features network self-construction and self–maintenance. It is composes of auto shared address, device localization and Log-in table. The network gateway node (the hub node) is capable of performing auto device pairing without any user interventions. This offers a large flexibility for users to add new device into the system and take the faulty devices out of the system on the runtime without any introductions and training.

This chapter introduces some general ideas to perform device pairing and device localization which have been studies theoretically or applied to commercial products, and describes the advantages and constraints of each pairing method. This offers a comprehensive understanding

of wireless devices management, a justification for the pairing method developed in this thesis; and will further benefit future developments.

A case study of ANT+ core wireless platform on a power wheelchair has been presented for demonstrating the auto device pairing. The network self-construction have been tested and demonstrated with two remote nodes.

Chapter 5 POWER MANAGEMENT

5.1 Power States Requirements

Power consumption is a key factor for commercialization of a wireless system. It is expected to allow years of operation without having to replace the battery for wireless communication. The power consumption depends on several factors, including wireless communication protocol, hardware design, message rate, serial interface and etc.

In the Section 3.1, an ultra-low power wireless communication protocol ANT has been selected. In this chapter, a power management method will be introduced to enhance the power conservation feature.

In a wireless network system over power wheelchair, the remote nodes are usually battery-powered and thus power constrained, while the hub node is powered by the main battery and considered as power of infinity. To conserve power, one principle is to assign power-consuming tasks to the hub and keep the remote nodes operate in low-power mode.

To minimize the power consumption, the system design should have a philosophy of minimal impact and minimal use. The protocol must transmit only what is going to be used, when it is going to be used. Transmission should be as short as possible to allow devices the most time in low power mode. The key benefits with this approach is not only to reduce the total amount of power consumed by wireless communication and also to free up the bandwidth for more devices to occupy the same frequency band.

To achieve this design goal, a design strategy is to manage the wireless mode in different device mode, and carefully design the power plan for each mode. The devices are able automatically change the way that they behave depending on the status of the system.

The device modes indicate how the device is working. They can be classified into four different modes in the wireless wheelchair system: shipping mode, idle mode, parking mode and active mode.

Shipping mode is applied while a wheelchair is stored in warehouse or transported to retailers. The system operates at ultra-low power in this mode, and it can tolerate slow wakeup up to two minutes.

Idle mode can be used when the device does not need to communicate with the system for a short period of time and wait in standby mode. It requires reduced power consumption and instantaneous wakeup when updating changes occur.

Parking mode, also called power-down mode, indicating that the system is shut down for a prolonged period of time. This mode can be applied while the users take sleep and etc. It requires very low power and can tolerate sluggish wakeup time up to 10 seconds.

Active mode is used while the system is operated, such as driving or seating. It requires all the operation-relevant nodes communication at full speed.

A wireless node is assigned into different device mode depending on the system status, the power states of the device is controlled by the host MCU using software commands and hardware interruptions. The transitions between different power states are defined according to the system requirements.

For a system, different sensors and user input devices are required for different operations. Operation modes can be used to optimize the power consumption to allow only operation-relevant devices be active when the system is implementing different operations, and other devices will keep in low power modes. When running a wheelchair, for example, some input devices may only control functions such as seating (e.g. changing the position or posture of the seating chair), in this case these devices can follow the idle mode rule while the wheelchair is driving. There are three different wheelchair modes:

- Drive mode – non driving sensors and input devices can be put into idle mode
- Seat mode – non seating sensors and input devices can be put into idle mode
- Docked mode (connected to a PC) – unused sensors and input devices can be put into idle mode

In this section, different power states and state transitions of ANT+ transceivers will be discussed. Details of development and implementation will be described. The power management of the MCU, in this case, the MSP430 microcontroller chipset is not the part of this section. One innovative approach for power management, the Master-Slave Swap mechanism is the emphasis in this section.

5.1.1 Power States and State Transitions

In system operations, the ANT devices will not transverse through these power states automatically. It is controlled by the host MCU using command messages or users interruptions. The triggering events for state transitions can be defined according to system requirements of different applications.

Figure 5-1 depicts that all power states and state transitions available in different device modes. The power states and the state transitions will be described in details in the following sections.

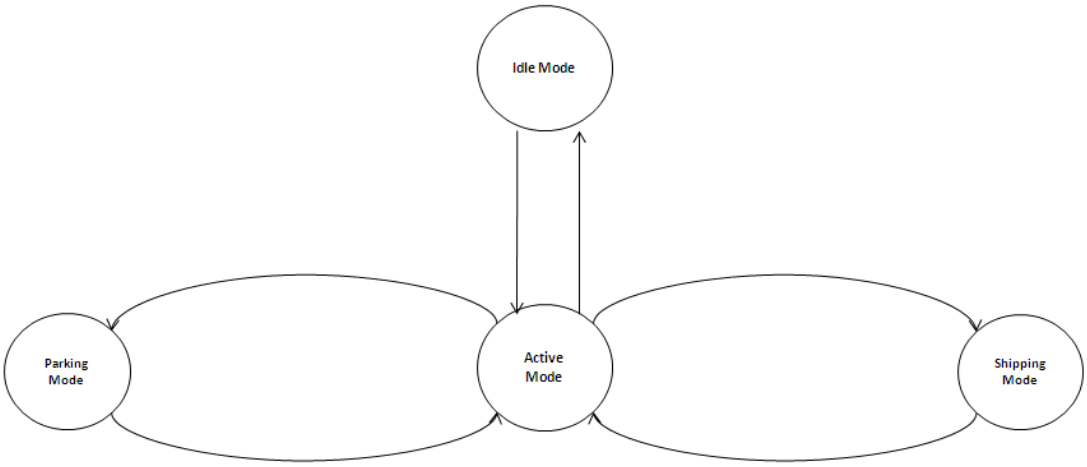


Figure 5-1 Power states and transitions.

One primary principle for power management development in this project is that, in a wireless control system, most remote nodes are not equipped with any user input interface, and users can only control the system through the hub node which has access for user interface. Thus, while the ANT of a remote node enters into a low power mode, it should be still able to receive incoming messages to accept power state transition messages from the hub node.

The ANT protocol has already provided power management module. However, they cannot be directly applied to the project to satisfy all the requirements. It requires the development of a full power management system based upon the power states provided in the protocol. Thus, it is helpful to review the power management embedded with ANT protocol first, and then we design a power management method based upon it and a novel power management method termed as Master-Slave-Swap will be introduced in Section 5.3.

5.2 ANT Protocol Power Management

The ANT protocol provides four power states for different applications. It can be implemented in either asynchronous mode or synchronous mode. The details can be read in [89], [90], [91]. Both asynchronous mode and synchronous mode refer to the interconnections between the ANT and the Host MCU. As there are two different serial interfaces available for ANT transceiver, and the power consumption and power management differ greatly for different interfaces. it is important to review each serial interface individually prior to developing a proper power management mechanism for wireless application on a power wheelchair.

5.2.1 Power States in Synchronous Serial Mode

The synchronous serial interface between ANT transceiver and the host MCU is shown in Figure 5-2. In this mode, the host MCU must be configured as a synchronous slave and the ANT

transceiver as a master. The synchronous serial interface can be used to interconnect with ANT and host MCU with hardware synchronous serial data link (synchronous messaging with byte flow control), e.g. Serial Peripheral Interface (SPI) or it can be simply maintained with I/O control when synchronous serial data link is not available on host MCU (synchronous messaging with bit flow control). In this section, only synchronous messaging with byte flow control is described, since power states and state transitions of bit flow control are identical to byte flow control, but more power consumption required for RF activities with bit flow control.

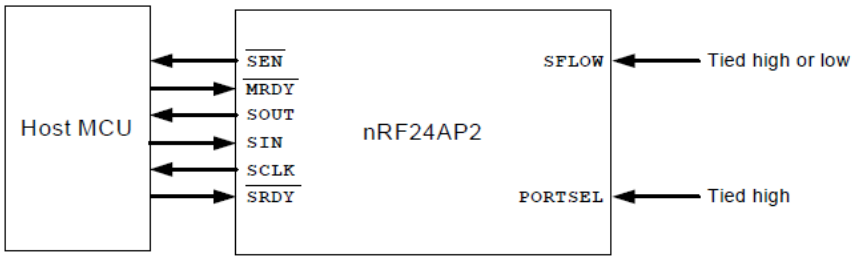


Figure 5-2 Synchronous mode interconnections [90].

The power states shown in Figure 5-3 are only available when running the ANT in synchronous serial mode.

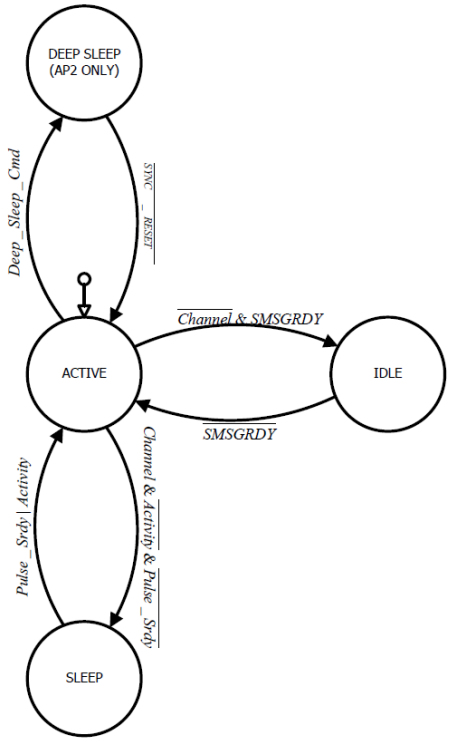


Figure 5-3 Possible power states and transitions in synchronous serial mode [88].

The operation mechanism of the synchronous mode interface is described in [91]. This is useful to briefly introduce it prior to understanding the power states and state transitions.

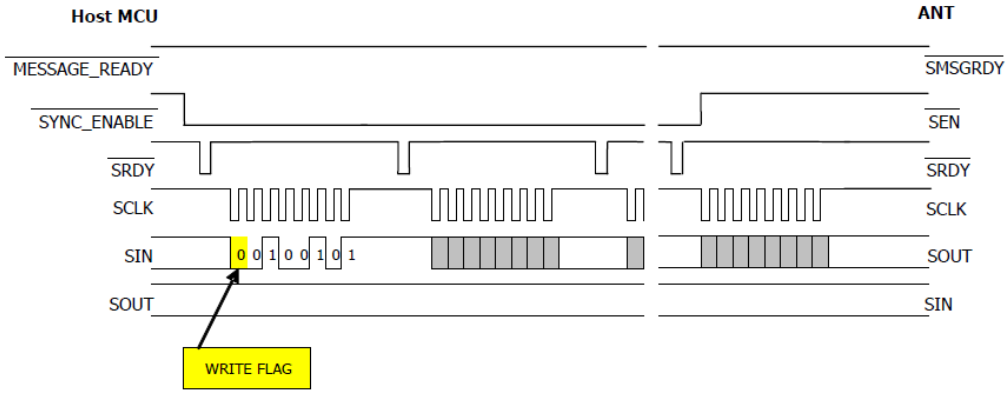


Figure 5-4 Transactions from ANT to Host MCU with software $\overline{SRDY}$ [90].

In Figure 5-4, it shows that the flow control in synchronous mode is controlled by $\overline{SRDY}$, $\overline{SEN}$ and $\overline{SMSGRDY}$ signals. For transactions from ANT to host MCU, $\overline{SEN}$ is asserted to indicate that the start of a message transfer, and $\overline{SRDY}$ is pulsed to signal its readiness for transactions of each byte. For transactions from host MCU to ANT, the operating mechanism is similar, the sole difference is that the $\overline{SMSGRDY}$ signal is asserted first to indicate that host MCU wished to transmit messages to ANT.

The power states transitions in synchronous mode are detailed in Table 7 [88]. The flow diagram of power states and state transitions are shown in Figure 5-3.

Transition	Description
pulse_srdy	$\overline{SRDY}$ signal pulse per byte
$\overline{SMSGRDY}$	Message ready signal is de-asserted
Activity	Incoming RF activity or events that need to be processed
Channel	At least one channel is open
SYNC_RESET	Synchronous Reset
Deep_Sleep_Cmd	Serial message command (message 0xC5)

Table 7 State transitions for synchronous mode.

To summarize the power states in synchronous mode, once the ANT has any channel remaining open, it can only operate in sleep or active states. ANT will transition to sleep state from active state automatically if any incoming RF event is detected by ANT and processed to host MCU by pulsing a $\overline{SRDY}$ signal to start the message transactions from ANT to host MCU. When ANT opens at least one channel and no RF event occur and no $\overline{SRDY}$ signal is asserted, ANT will remain in sleep state.

When ANT operates in idle or deep sleep state, all the channels will be closed, ANT will not receive any RF messages and the host MCU is not able to send any message to ANT. The only

difference between these two states is that the device does not need to erase all the channel configurations while it is in idle state. However, all the channel configurations will be cleared and require synchronous reset of the device when it transitions into active state from deep sleep state.

The synchronous reset is required to guarantee synchronization of synchronous serial port any time the device is powered up or it loses synchronization. The synchronous reset can be implemented in several different methods. The first method is hardware reset. It is only available when a reset pin is available on the chipset, ANT will be reset by asserting a reset signal via the reset pin. The second method is software reset. It simply passes a reset command message (0x4A) from host MCU to ANT via serial interface. This method is only applicable after communication has already been synchronized, but not applicable in power up state. The third method is to reset ANT by applying a specific sequence which is shown in Figure 5-5 [89]. This synchronization reset method will be applied for state transitions from the deep sleep to active state as it does not require any hardware interruption and it can be applied in power up state.

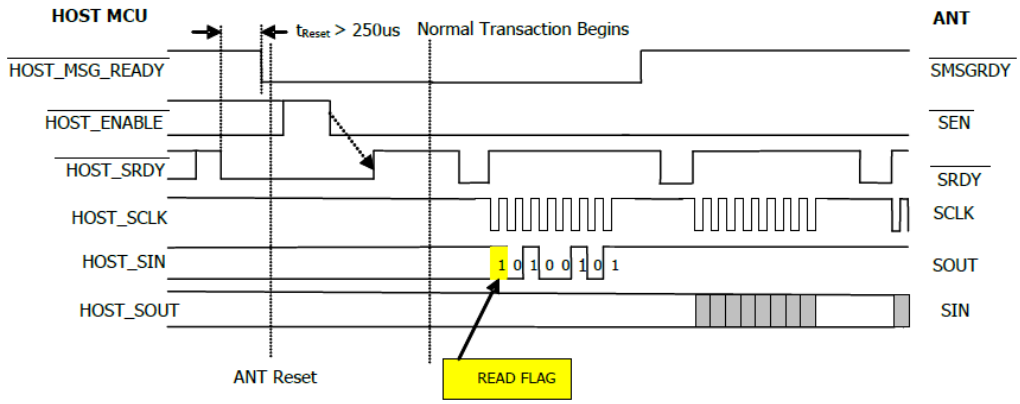


Figure 5-5 Synchronization with ANT [89].

The synchronization reset method in Figure 5-5 can be interpreted by pseudo codes shown below:

```
SYNC_SMSGRDY_DEASSERT();      //de-assert SMSGRDY signal (SMSGRDY = 1)
Timer_DelayTime(2 ms);        //a 2 mini-seconds delay
SYNC_SRDY_ASSERT();           //assert SRDY signal (SRDY = 1)
Timer_DelayTime(300 us);      //a 300 micro-seconds delay
SYNC_SMSGRDY_ASSERT();        //assert SMSGRDY signal (SMSGRDY = 0)
Timer_DelayTime(2 ms);        //a 2 mini-seconds delay
SYNC_SRDY_DEASSERT();         //de-assert SRDY signal (SRDY = 0)
Return (if SEN == 0);         //wait until SEN is asserted
```

The flow control during this synchronization reset process can be illustrated in Figure 5-6 .

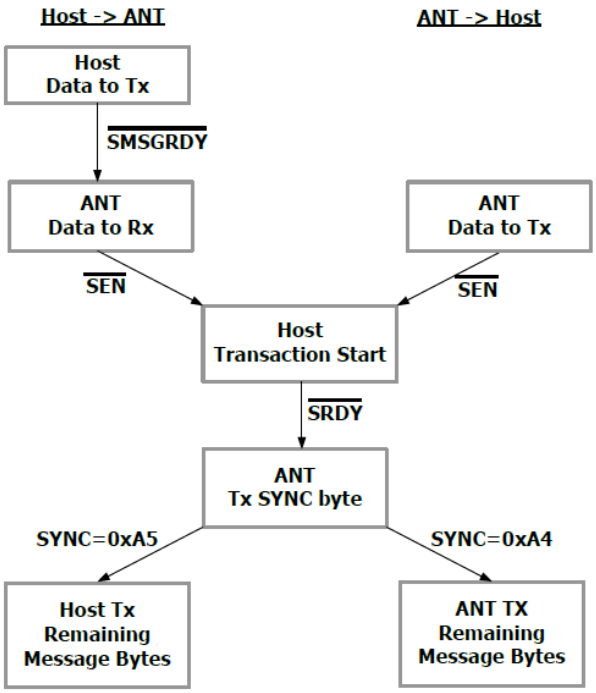


Figure 5-6 Synchronization serial communication [91].

Note that the SMSGRDY signal must be de-asserted for sufficient period of time to wait for ANT to finish power up and get ready for incoming messages. Otherwise the ANT will not transmit the first message properly. The first message is a SYNC message, and it is always transmitted from ANT to the host MCU and used to indicate the direction for communication in the serial interface port. It can be either 0xA4 or 0xA5, with the least significant bit indicating the direction of the remaining bytes (0: messages receive from ANT to host MCU; 1: messages transmit from host MCU to ANT). The synchronization can be accomplished only when the SYNC message is received, the ANT will not return a SYNC message if the SMSGRDY signal is not de-asserted for enough time.

In this section the power states and state transitions of synchronous serial interface are introduced. The following section will briefly describe those of asynchronous serial interface, so to compare the power managements with different serial interface and thus determine an optimal way to conserve power.

5.2.2 Power States in Asynchronous Serial Mode

Asynchronous serial interface is usually applied for interfacing ANT with host MCU which is not equipped with synchronous serial hardware. The interconnection between host MCU and ANT is shown in Figure 5-7 [91].

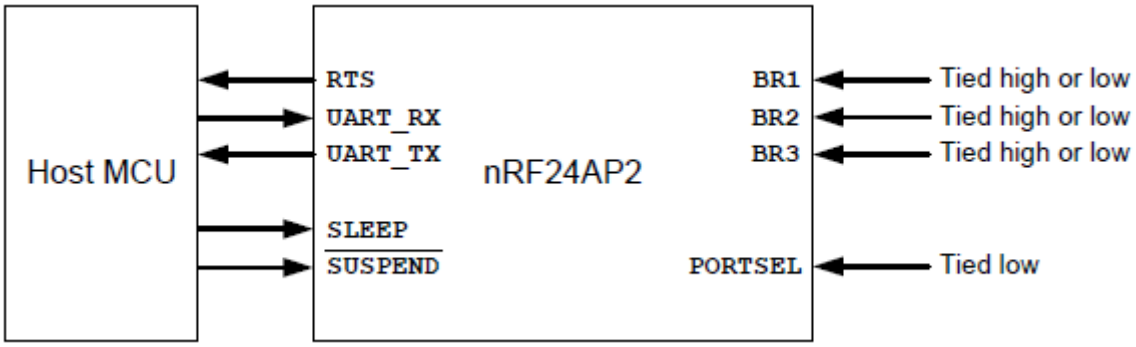


Figure 5-7 Asynchronous mode connections [91].

The baud rate of the asynchronous interface between host MCU and ANT can be configured from 1200 to 57600 baud. Flow control of asynchronous mode is performed by the RTS signal. The power states and state transitions are shown in Figure 5-8.

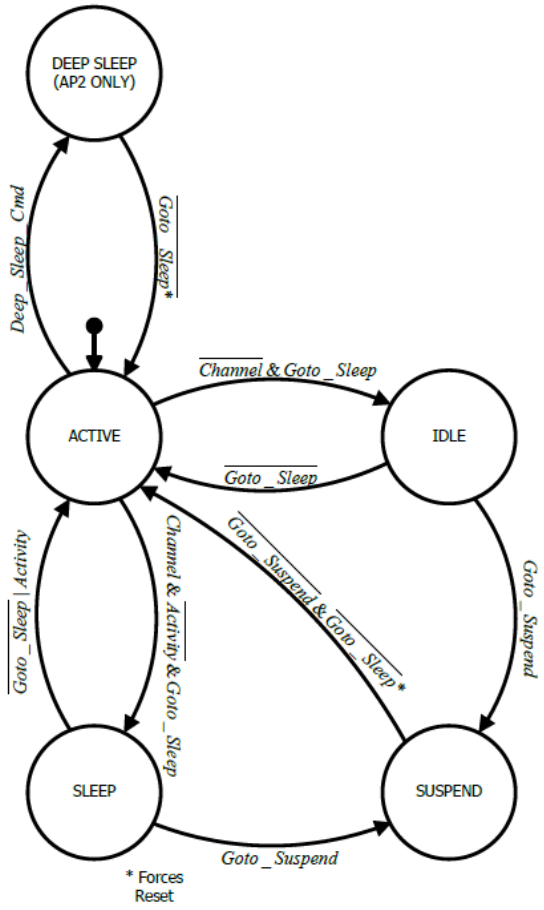


Figure 5-8 Possible power states and transitions in asynchronous serial mode [88].

Figure 5-8 depicts all the possible power states and state transitions for asynchronous mode. The suspend state is the only one that is not available in synchronous mode. However, the

other four transition states differ from those for synchronous mode, and are summarized in Table 8.

Transition	Description
Goto_Sleep	$SLEEP$ signal asserted (active high)
Goto_Suspend	$SUSPEND$ signal asserted (active low)
Activity	Incoming RF activity or events that need to be processed
Channel	At least one channel is open
Deep_Sleep_Cmd	Serial message command (message 0xC5)

Table 8 State transitions for asynchronous mode

The differences of power management modules between asynchronous interface and synchronous interface are caused by the flow control mechanism. In asynchronous mode, host MCU uses $SLEEP$ and $SUSPEND$ signals to allow ANT to enter into sleep and suspend mode which helps conserving power consumption. This power state is not available in synchronous flow control.

The suspend state can be considered as an intermediate state and allows ANT to enter a low power state from either idle state or sleep state. In the suspend state, all RF activities will be terminated and ANT will be reset while entering into or taking out of the suspend state. This state is useful for applications that require suspend functionality such as USB stick.

Power states and state transitions for asynchronous mode and synchronous mode have different characteristics and should be used for different applications. It is useful to understand the differences between them, and which one should be the optimal for application of wireless control for a powered wheelchair.

5.2.3 Comparisons of Power Management Methods between Asynchronous Mode and Synchronous Mode

The serial interface does not make significant difference in power consumption. The current consumptions for different modes do not change for the given state in either asynchronous mode r synchronous mode [88]. The details are shown in Table 9.

Power State	With 32 kHz External Clock		Without 32 kHz External Clock	
	Synchronous	Asynchronous	Synchronous	Asynchronous
Active	~3 mA	~3 mA	~3 mA	~3 mA
Suspend	N/A	2 uA	N/A	2 uA
Sleep	3 uA	3 uA	100 uA	100 uA
Idle	2 uA	2 uA	2 uA	2 uA
Deep Sleep	0.5 uA	0.5 uA	0.5 uA	0.5 uA

Table 9 Current consumptions in different power states.

The presence of external 32 kHz clock has significant impact on power consumption in both modes. This is because the 32 kHz clock has to be synthesized from the internal clock if external

clock is not used, this will increase the current consumption. Table 10 shows that such impact is significant for ANT running in sleep state, but it is negligible for other power states. This is because, in active state, the current consumption for clock synthesis makes only slight increase to total current consumption, and for deep sleep and idle states, all the peripheral clocks will be disabled, the clock synthesis will not take any action. The average current consumption for message reception and transmission with different interfaces is shown in Table 10. More details can be found in the data sheet [92]. When running ANT in synchronous mode, it always requires less current consumption. And for asynchronous mode, the average current consumption usually decreases with higher baud rate.

Conditions	Average Current Consumption (uA)
Average current per Rx message in sync mode byte flow control	21
Average current per Rx message in async mode at 57600 baud	22
Average current per Rx message in async mode at 50000 baud	25
Average current per Tx message in sync mode byte flow control	27
Average current per Tx message in async mode at 57600 baud	40
Average current per Tx message in async mode at 50000 baud	45

Table 10 Average current consumption for different applications and different interfaces.

Another major difference is that the suspend state is not supported in synchronous mode. The suspend state is useful for the applications that require suspend functionality. However, for applications of wireless control on a power wheelchair, the suspend functionality is not required. Hence it will not make any impact for such an application.

Sleep state is the only low power state that still allows ANT to open channel and receive RF messages for both synchronous and asynchronous modes. However, the operating mechanism is different. In asynchronous mode, the sleep state is controlled by the $SLEEP$ signal. ANT will halt any transmission from host MCU to ANT once $SLEEP$ signal is asserted. However, transmission from ANT to host MCU will remain in the active state, regardless of the status of $SLEEP$ signal. This can be illustrated in Figure 5-9(a). While $SLEEP$ signal is asserted, serial interface transmission from the host MCU to the ANT transceiver is disabled, the ANT transceiver will send message to the host MUC when available, regardless of the state of $SLEEP$ signal.

In synchronous mode, sleep control is different: all the state transitions in synchronous mode are automatic, which means no interruption from the host MCU will be required to change the power state. In contrary, it is up to the host MCU to control the state transitions in asynchronous mode. This is illustrated in Figure 5-9(b), ANT transceiver will automatically transition into the sleep state at any time it is waiting for an $\overline{SRDY}$ pulse and return to the active state while an $\overline{SRDY}$ signal is pulsed and an RF event is detected. For each time an $\overline{SRDY}$ signal is pulsed, the serial clock signal will be activated to start serial interface communication and deactivated (tied to high) while one byte serial message has been

completed. The ANT transceiver will then remain in the idle state until the next $\overline{SRDY}$ pulse. During the sleep state, the host MCU will not be able to receive or transmit serial messages to the ANT transceiver.

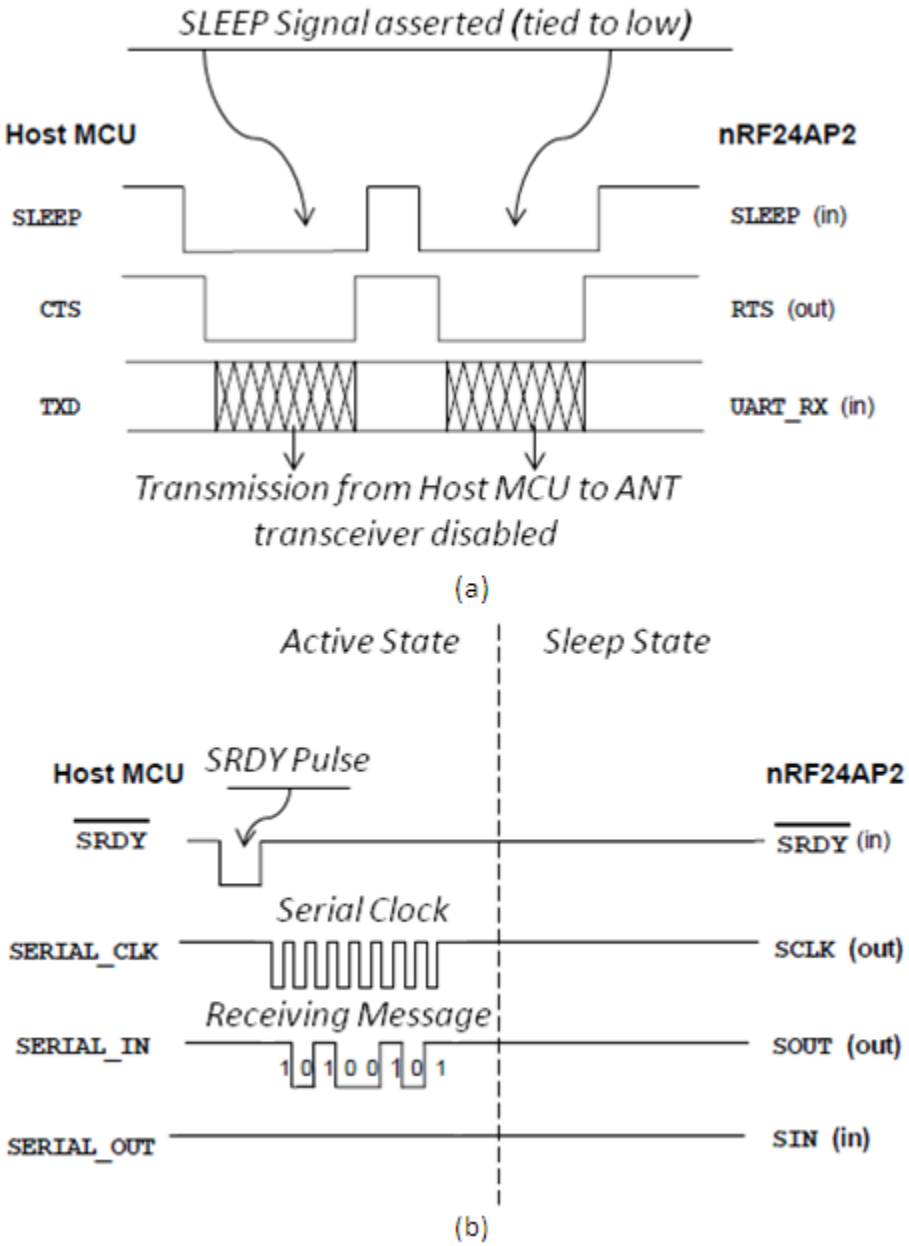


Figure 5-9 Sleep control in asynchronous and synchronous modes

Resetting ANT in asynchronous mode is different from that in synchronous mode. Resetting in synchronous mode has been described Section 5.2.1, with three different methods. In asynchronous mode, ANT provides a special method which is available in asynchronous mode only. In Figure 5-8, it is shown that ANT can only enter into suspend state from either idle or sleep state. If $SUSPEND$ signal is asserted while running ANT in active state, ANT will be reset immediately, as shown in Figure 5-10 [88].

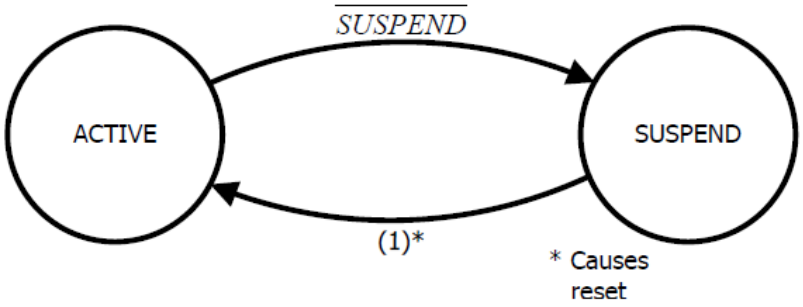


Figure 5-10 Resetting ANT using $SUSPEND$ signal.

Unlike asynchronous mode, transitions into deep sleep state do not require additional timing constraints in synchronous mode. In synchronous mode, ANT can enter into the deep sleep state by simply sending deep sleep command messages. In asynchronous mode, to enter into the deep sleep state, the $SLEEP$ signal must be asserted within 1.2 ms after the deep sleep command message (0xC5) is sent to ANT, which is shown Figure 5-11.

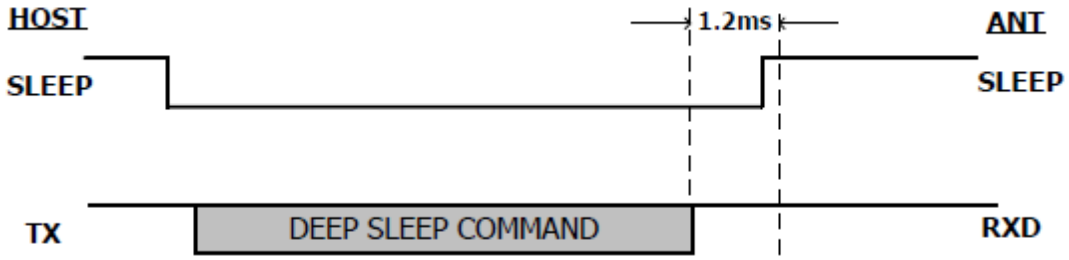


Figure 5-11 Deep sleep control in asynchronous mode.

In this section, some differences for power managements between two different serial interfaces between host MCU and ANT has been introduced. Some of these differences will not have significant impact on the applications for wireless control on a power wheelchair, and others should be taken into account for developing a proper power management for such an application.

5.2.4 Choice of Synchronous Serial Interface

Requirements of power management for the applications of wireless control on a power wheelchair have been described. Requirements of different power states and state transitions have been determined in different scenarios according to the application. Now it is crucial to take further research to find the gaps between project requirements and power management supported by ANT wireless protocol, and thus to determine the methodology to fill the gaps.

The first step to achieve this goal is to determine a proper serial interface for such an application. The comparisons between power managements in synchronous mode and asynchronous mode have been described. To determine which one is a more proper serial

interface for this application, two primary factors need to be considered: 1) power consumption and 2) ease of state transitions control.

Power consumptions are almost the same in different serial interfaces, as listed in Table 9. From Table 10, it is shown that power consumption in synchronous mode is slightly less than that in asynchronous mode, in the measurement of micro-amperes. However, the slight difference in power consumption can be accumulated to large amount over long time period.

For state transitions control, ease of control refers to quick response and reliable transitions. State transitions in synchronous mode is more automatic, requiring control over serial signals such as $\overline{SMSGRDY}$ and $\overline{SRDY}$. In asynchronous mode, extra controls over $SLEEP$ and $SUSPEND$ signals are required for ANT to transverse through different power states.

The asynchronous serial port provides the unique suspend state. It is quite useful for applications that require suspend functionality (such as USB stick). However, for applications in this project, it is not necessary.

To summarize the power management provided by ANT wireless protocol, the synchronous serial interface consumes less power and provides ease of state transitions control, which is considered to be a more proper interface for this project.

5.3 Master-Slave Swap Operation

To understand the Master-Slave Swap (MSS) operation, it is quite important to introduce some features of ANT wireless protocol. With ANT protocol, a wireless communication channel is built between two nodes, as shown in Figure 5-12.

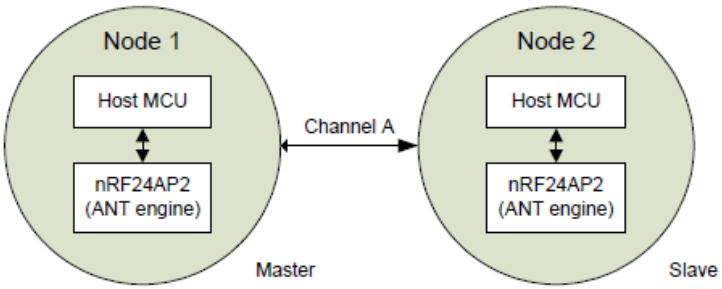


Figure 5-12 ANT nodes and the channel between them.

To establish a wireless channel, one node has to be configured as a master node and the other one as a slave. Master node controls timing of a channel, which means, for each data transmission, the master node will initiate the communication by sending an addressed message to the slave node, and the slave node can optionally transmit a message in the reverse

direction after it receives the message from the master node. This feature results in more power consumption: for a slave node to send an RF message to a master node, it always requires one reception and one transmission, which can double the power consumption or even more.

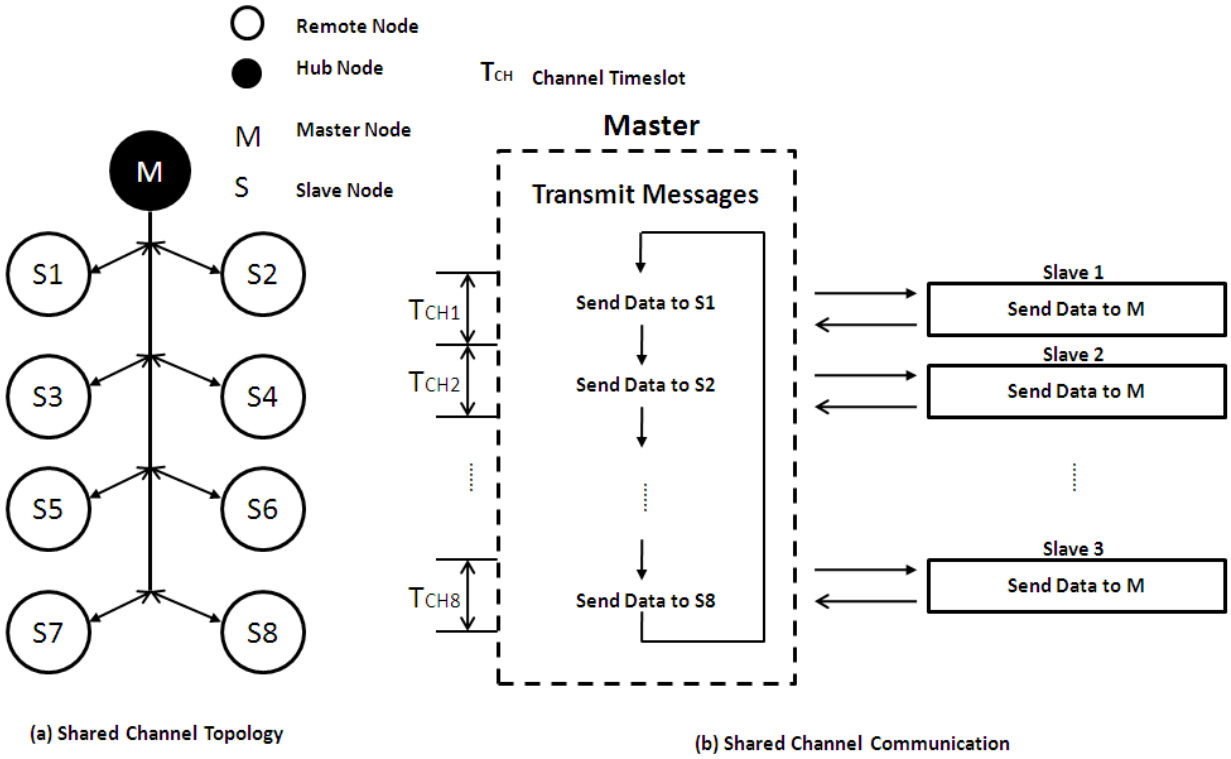


Figure 5-13 Shared channel topology and communication.

In this project, when running the system in active mode, shared channel topology is used, as shown in Figure 5-13 (a). In this network topology, the hub node is configured as the master node and remote nodes act as the slave nodes. The advantage of this configuration is that the hub node is able to allocate time period to each remote node in the network and cycle through each remote node for wireless communication, as shown in Figure 5-13 (b). The hub node is connected to the main battery of the wheelchair as a gateway node, which can be assumed to be power infinite. The remote nodes are all battery powered, which is power constrained.

Shared channel topology takes advantage of ease of control at the expense of more power consumption. If remote nodes can be configured as the master nodes and the hub node act as slave node, they will be able to send RF messages to the hub without having to listen to the channel for receiving addressing messages from the hub, resulting in a significant reduction in power consumption for remote nodes. By this means, the network will be re-configured as a one-slave, multi-master topology.

The ANT wireless protocol provides continuous scanning mode to allow a slave node to receive messages from multiple master nodes [93]. This can be utilized as the foundation for the

development of MSS. The continuous scanning mode will be introduced first, followed by one section to describe how it will be applied for conserving power for the wireless network in this project, how MSS can be developed based upon the continuous scanning mode and finally the implementation of it.

5.3.1 Continuous Scanning Mode

The continuous scanning mode refers to configuring an ANT node in scanning mode to continuously listen to the channel and receive messages from multiple nodes at any time. The network topology is different from the shared channel, as shown in Figure 5-14 (a).

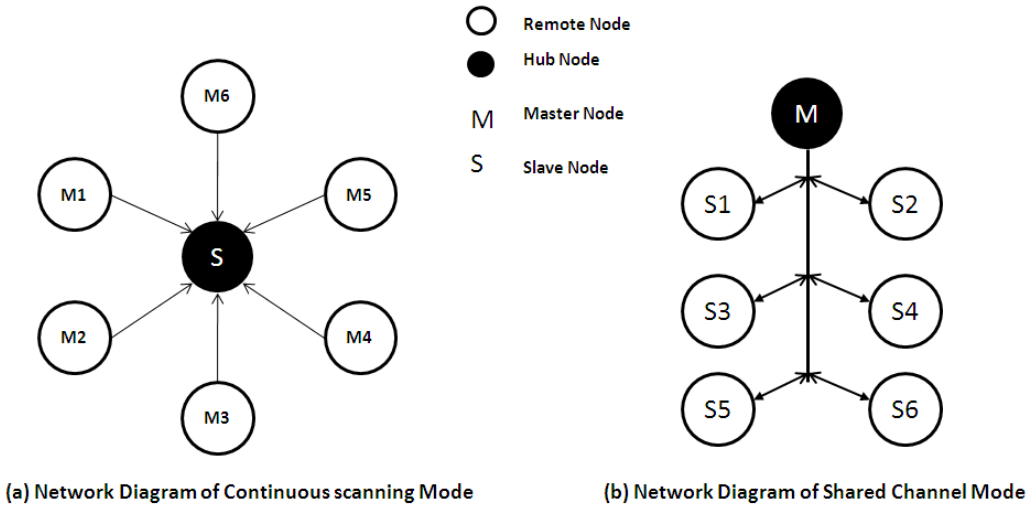
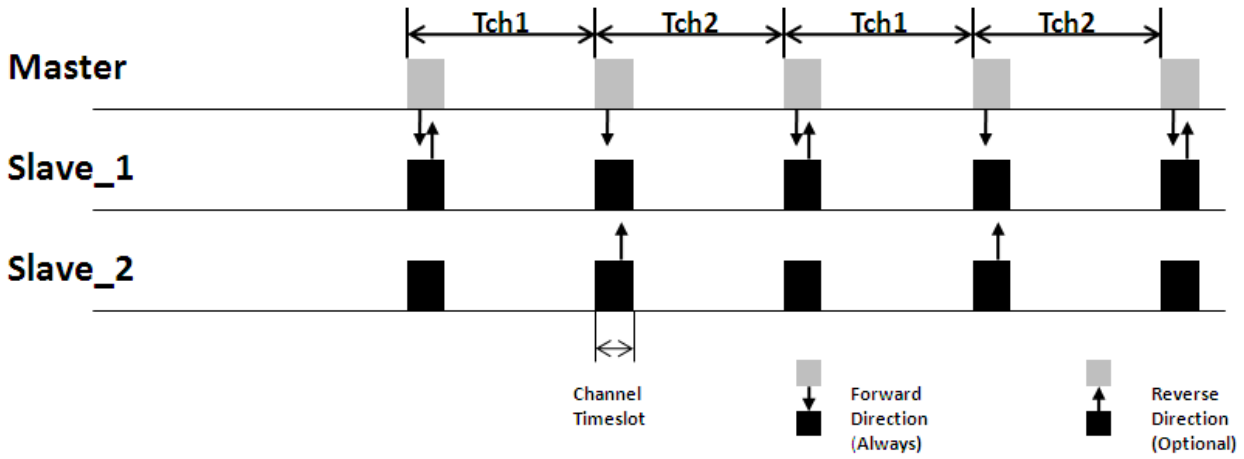
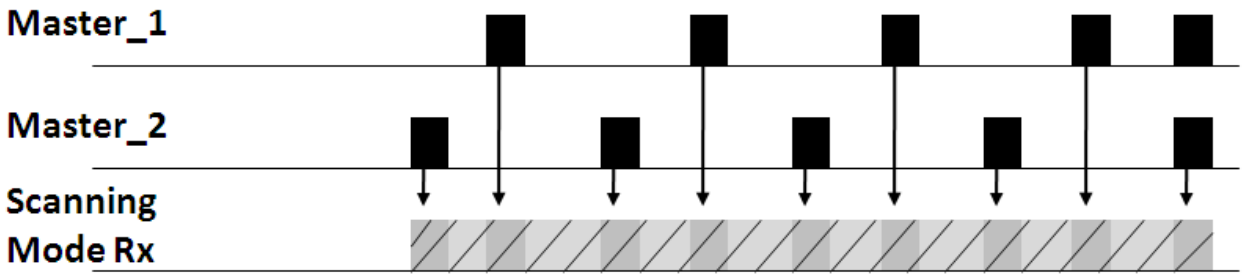


Figure 5-14 Network diagram.

In a shared channel mode as shown in Figure 5-14 (b), a master node controls timing of all the remote nodes in the network and cycles through each node by polling operation. All the channels are operated in synchronized fashion. However, in the continuous scanning mode, a central slave node remains active to listen to the channels and receive messages at any time. The comparison of these two different modes is shown in Figure 5-15.



(a) Operation of shared channel mode



(b) Operation of continuous scanning mode

Figure 5-15 Network operations

It is shown that the operation mechanisms differ between the two network structures. In the shared channel mode, channel operations are performed in a synchronous fashion, RF events only occur in each channel period. However, in continuous scanning mode, a master node can transmit any time it wishes to send a message. This results into two different modes for triggering the node: event-driven mode for the continuous scanning mode and schedule-driven for the shared channel mode, shown in Figure 5-16.

Note that in the schedule-driven mode, the hub node triggers each remote node by sending addressing messages in each message period to avoid channel collision. In the event-driven mode, the remote node will send data message whenever available, and the hub node receives the message without the latency associated with channel acquisition on synchronization in the shared channel mode. However, if too many remote devices operate in the networks simultaneously, the odds of channel collision will increase, and the remote nodes will have to retransmit the messages if they have not been transmitted successfully. This can increase the system latency and power consumption. A mathematical model is built to compare the power consumption with these two different operation modes, the details are described in Section 5.5.

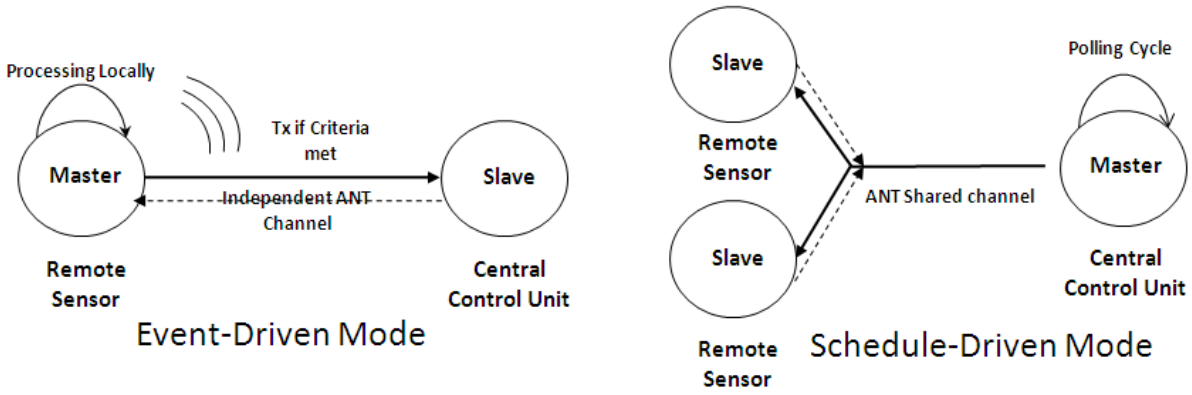


Figure 5-16 Two different modes for node triggering.

In continuous scanning mode, the central node is configured as a slave node and always operates in continuous scanning mode, thus it consumes significant power (~ 18 mA). Hence, the central scanning node should be powered by a source with sufficient power capacity. In this project, the continuous scanning mode is running on the hub node which is connected to the rechargeable main battery, with large power capacity.

The continuous scanning mode offers the advantages of conserving power. However, the shared channel mode has the advantages of precise channel timing control, especially when a network runs at high data rate. Hence, the network needs to swap modes between the continuous scanning mode and the shared channel mode to capitalize on the benefits of both operation modes according to the requirements of the operation scenarios. Such a swap operation method denoted as Master-Slave Swap, is the key to energy-efficient operation of the wireless network on the power wheelchair. It implies that all the nodes need to be reconfigured from master to slave or vice versa.

5.3.2 Master Slave Swap Handshaking

Assume that a network is self-constructed in the shared channel mode, and it wishes to transition into the continuous scanning mode. To complete such an operation, a handshaking procedure, denoted as Master Slave Swap (MSS) handshaking, must be devised.

To perform the continuous scanning mode, the central node requires several steps for configuration, as shown in Figure 5-17.

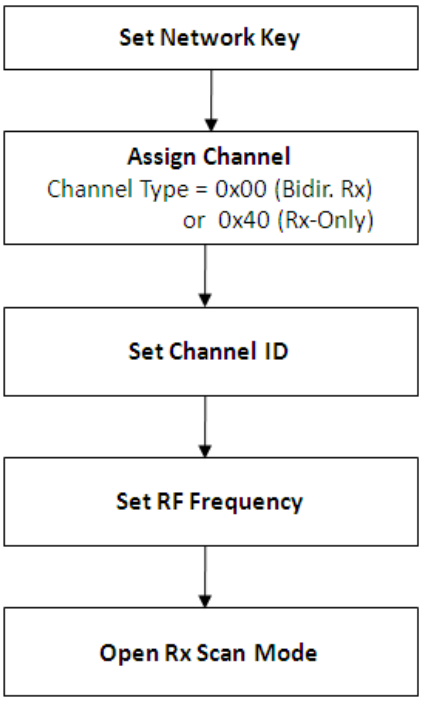


Figure 5-17 Scanning mode Setup for the hub node.

Note that the central hub node operates in channel 1 after auto pairing is completed. However, the continuous scanning mode can be only performed in channel 0. Thus, it requires channel 0 to be opened and all other channels to be closed, since the continuous scanning mode makes full use of the radio. While running the continuous scanning mode with any other channel open, ANT will send a CLOSE_ALL_CHANNELS (0x19) message to indicate that it is an invalid attempt. And since channel 0 has been already been configured for the shared channel mode, a procedure for channel reconfiguration has to be executed prior to opening the continuous scanning mode.

As the first step, the hub node determines to start MSS when it accepts a triggering event, e.g. a user command. Then it keeps sending broadcast messages to all the remote nodes in the network to inform them to take actions for MSS. To complete MSS, back and forth communication takes place between the hub and remote nodes, which is shown in Figure 5-18.

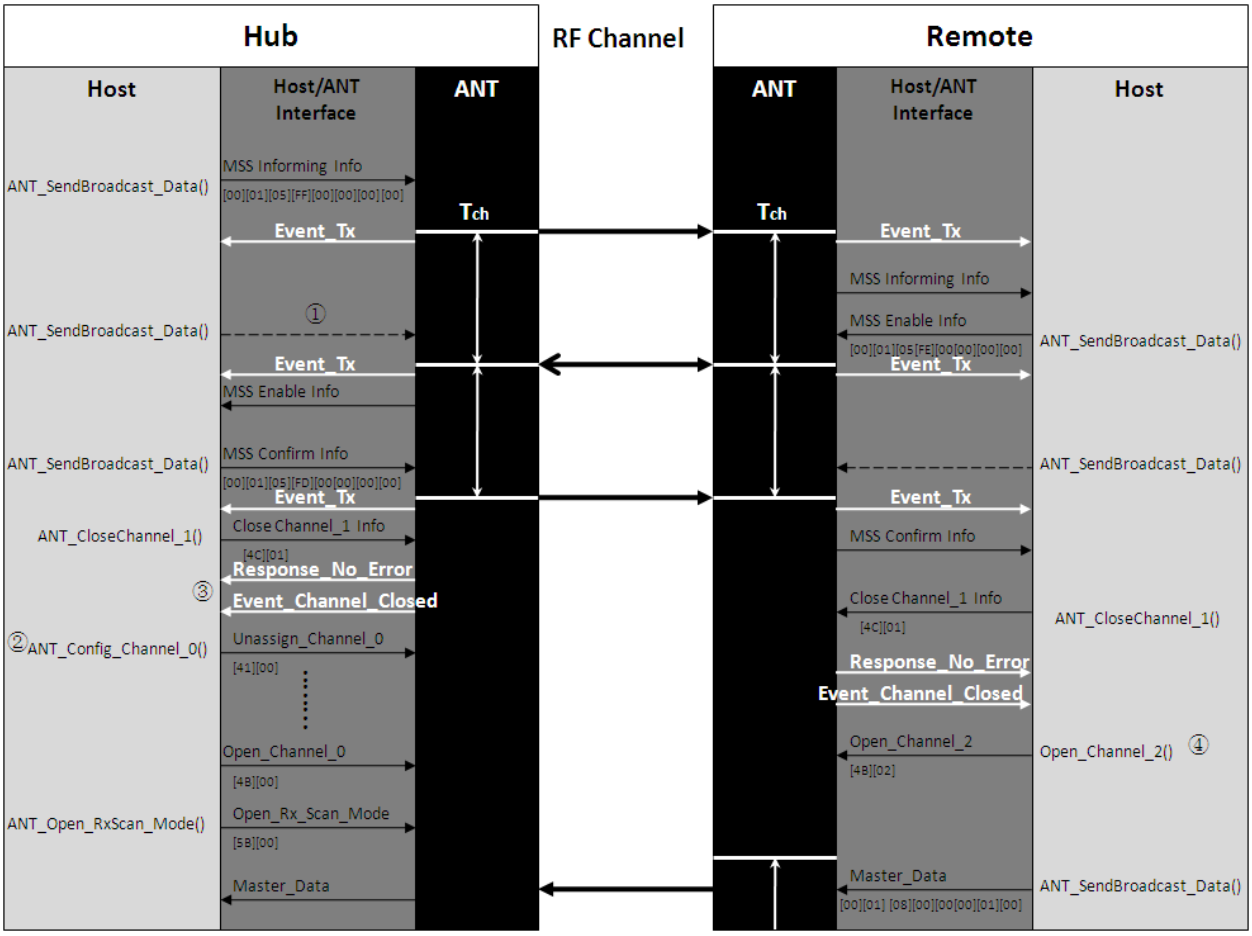


Figure 5-18 MSS sequence diagram.

Note that:

① Arrows in dashed line represent automatic messages. While host MCU does not send to ANT any message to transmit, ANT will automatically repeat transmission of the message which has been transmitted in the previous time slot.

② Channel configuration for ANT channel involves a set of command messages from host MCU to ANT to define all the configurations required for channel setup, the details can be found in [94].

③ ANT_CloseChannel message is sent to close a channel which has previously opened. The host will indicate that the message has been received by ANT while a Response_No_Error (0x00) message is received. However, the channel will not be successfully closed until the host receives an Event_Channel_Closed (0x07) message.

④ For a remote node, channel_2 has been previously configured for operations in the continuous scanning mode. Thus, during the procedure of MSS handshaking, it simply opens the channel_2 instead of configuring channel_0.

Figure 5-18 shows a scenario that how MSS is performed to transition from the shared channel mode into the continuous scanning mode. The MSS handshaking procedure starts by the hub node broadcasting a message MSS_Informing_Info to inform a remote node that the system wishes to enter into the continuous scanning mode. The remote node then indicates that it has received the informing message by sending back an MSS_Enable_Info message. The hub node indicates the completion of MSS by broadcasting an MSS_Confirm_Info message when the MSS_Enable_Info message has been received. Then the hub closes all other channels, in this scenario the channel 1; and reconfigures channel 0 for the continuous scanning mode. Note that the reconfiguration of channel 0 begins with ANT_Unassign_Channel_0 message (0x41). This command message is only required for configuring a channel which has been previously configured: even the channel has been closed, the channel configuration remains and must be unassigned prior to reassigning it. During the reconfiguration procedure, the channel will be configured as a slave receive channel, either receive-only channel (0x40) or bidirectional-receive channel (0x00), as shown in Figure 5-17. The reconfiguration of channel 0 ends up with ANT_OpenChannel_0 message, which indicates that the channel has been setup for the continuous scanning mode, and the command message ANT_Open_Rx_Scan_Mode (0x5B) is sent to open the continuous scanning mode. The hub will be always active and pick up any message, regardless of time period.

Following the initiation by the hub node, the remote node closes channel 1 and opens channel 2 once it receives MSS_Confirm_Info message. Channel 2 has been previously configured as a bidirectional master channel, with all other fields retaining the initial configurations that have been assigned during the auto paring procedure. Once channel_2 has been opened, the remote node will immediately broadcast messages. However, these messages cannot be received by the hub node if the channel setup has not been completed at the hub node end.

In Figure 5-18, the remote node sends data message to the hub after the continuous scanning mode has been enabled. Note that the data message has a unique shared address 0x0001, to allow the hub node identify the source of each message. The data type is 0x08 which is defined for heart-beat message, which is used for informing the presence of the remote node and used for the hub node to maintain the RF link while low power mode has been applied. The seventh byte (0x01) is the information byte that carries the information collected at the remote end and required by the hub node.

The handshaking message starts with the shared channel address (0x0001) which is inherited from the auto device pairing procedure, followed by the data type byte (0x05) which is reserved for indicating that the message is used for MSS handshaking messages. Two CMD bytes are specified for command information, indicating the stage of the handshaking procedure. These handshaking messages are user-defined to control the handshaking procedure. The message format is shown in Table 11, with the example that the shared address is previously configured as 0x0001:

Source	Source	Type	Shared Address	Data Type	CMD	Data_1	Data_2	Data_3
Hub	MSS Inform	Broadcast	[00][01]	05	FFFF	00	00	00
Remote	MSS Enable	Broadcast	[00][01]	05	FFFE	00	00	00
Hub	MSS Confirm	Broadcast	[00][01]	05	FFFD	00	00	00
Remote	Master Data	Broadcast	[00][01]	08	0000	00	01	00

Table 11 User-defined RF handshaking messages for MSS

The state machine shown in Figure 5-19 illustrates how the MSS is progressed at both hub and remote ends, and the conditions for state transitions.

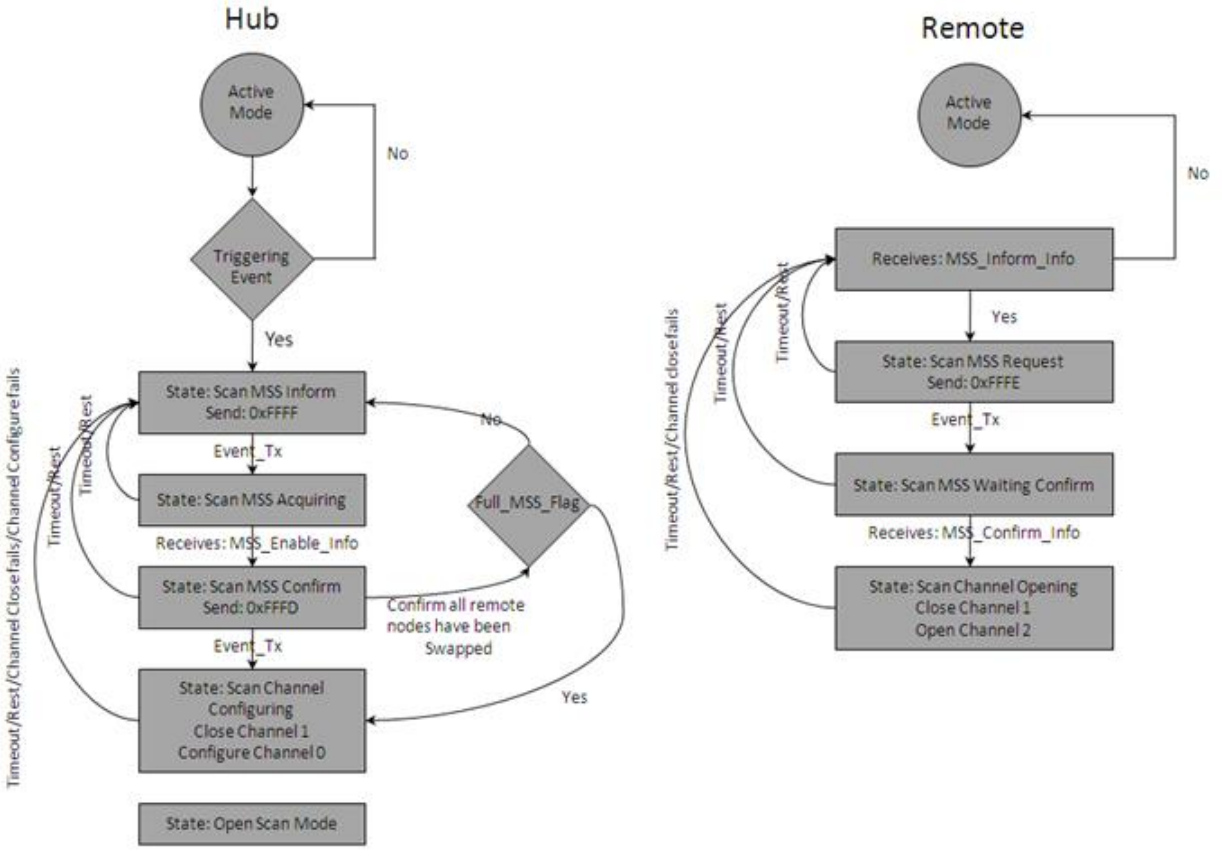


Figure 5-19 State Machine for MSS

Note that the remote node has been configured with shared address 0x0001 and both ends start MSS from active mode. The triggering event for MSS at the hub end could be defined as user operation (e.g. button) or automatic control (e.g. remains idle for a certain time period). The remote node enters into MSS while it receives an MSS_Inform_Info message that matches its shared address.

The remote node will open a master channel and swap into master mode once it receives MSS_Confirm_Info message. However, for the hub node, it will cycle through all the remote nodes in the network prior to closing all other channels and configuring the channel_0. A full_MSS_flag will be flagged if the hub confirms that MSS for all the remote nodes have been completed.

Running the wireless communication in the continuous scanning mode can minimize the power consumption for the remote nodes. However, since communications are performed in asynchronous fashion, channel congestion may occur with a higher probability especially in the presence of a large number of remote nodes. This issue needs to be taken into account and further researched for utilizing MSS for power management on a power wheelchair.

In this project, MSS is only developed and tested for a peer-to-peer scenario. For MSS operations for one-hub, multi- remote structure, the scanning node is able to support a number of simultaneous transmissions. The maximum number of simultaneous transmissions is limited by the available bandwidth of the scanning node and the resources provided by the host MCU on the scanning node. The ANT+ protocol can tolerate up to 300 nodes at 1 Hz transmission rate in the same RF space [95]. In an ANT network, for operations in a shared channel mode, master device performs channel management for synchronous channelization, so that transmissions from different slave nodes are able to coexist with each other in a given RF space. However, transmissions in the continuous scanning mode are performed in an asynchronous nature. The scanning mode is active at full time and receives messages from any master device regardless of its channel period, which means transmissions from multiple master nodes may collide with each other. It is important to perform channel management to synchronize transmissions from all the master devices after MSS is performed, so that transmissions from each master device only occurs only in the channel period that has been allocated to it. The development of channel management for the continuous scanning mode is not included in this thesis, but a part of future development.

5.4 Implementations of Power Wheelchair with Developed Power Management Module

The power management module is developed based upon ANT+ protocol, and targeted to satisfy the requirements of power states and state transitions for a power wheelchair. The power states and state transitions requirements are described previously. In this section, a case study will be conducted to illustrate how the power management will be performed for a power wheelchair. Note that the serial interface between ANT and host MCU is synchronous mode with byte flow control.

As described previously, in a wireless control network for a power wheelchair, a node has four power modes: shipping mode, parking mode (or power down mode), idle mode and active mode. A distance sensor is taken as an example for interpreting how the sensor operates within each power state and how the state transitions will be performed.

Assume that a wheelchair is operating in drive mode, and the distance sensor is operated in active mode for collision avoidance purpose. Assume that the wheelchair is mounted with ten wireless sensor nodes and four of them are drive-relevant. Hence, the hub node will cycle through four remote nodes during each polling cycle, the distance sensor receives an addressing message from the hub node and transmit back data message which contains distance information it has collected. This can be illustrated in Figure 5-20.

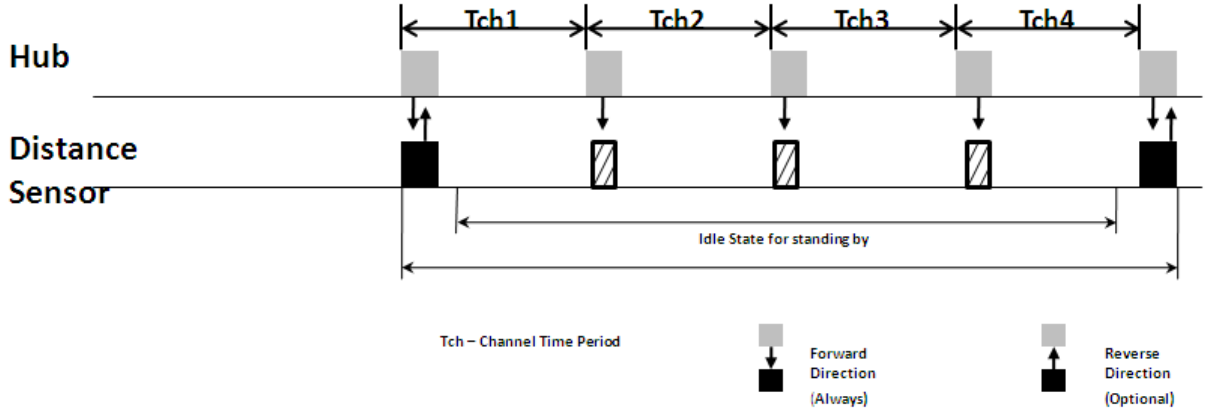


Figure 5-20 Operations of distance sensor in active mode.

Note that while the network operates in shared channel mode, the communication between a master node and a slave node is performed in synchronous nature. While all channels are closed on the slave side, the slave node will lose synchronization response in a very short period of time and thus not response to any RF events or command messages from the host MCU, acting as completely “dead”. Thus, for wireless communications in the shared channel mode, the slave node has to receive an addressing message in each channel period to maintain its synchronization, otherwise it will lose channel link to the hub in a short period. However, the slave node may choose not to send back data messages to the hub node during the channel period that the hub node sends addressing messages to other slave nodes within the network. This can be achieved by simply sending a null message at the slave side, Figure 5-21 shows the transitions that a slave node transitions from the active mode to the idle mode with such an approach. Note that sending a null message can only disable RF transmission on a slave node. For a master node, ANT transceiver will automatically retransmit the previous message if null message is sent from the host MCU. For a master node, the only way to disable RF transmission is to close all the channels on it. The average current assumption will significantly decrease from 380 micro-amperes to 220 micro-amperes while the power state transitions from the active mode to the idle mode. The details will be described in Section 5.6.

As shown in Figure 5-20, the distance sensor will transition into the idle mode channel every time that RF communication completes and remains in the idle mode for four time periods, and

only transmit data messages back to the hub node in the designated time period for it. During the idle state, the remote node will not transmit any message in the reverse direction and only listen to the channel for maintaining the channel synchronization. The remote node will enter into active state only when the shared address field of the addressing message it receives matches its assigned shared address.

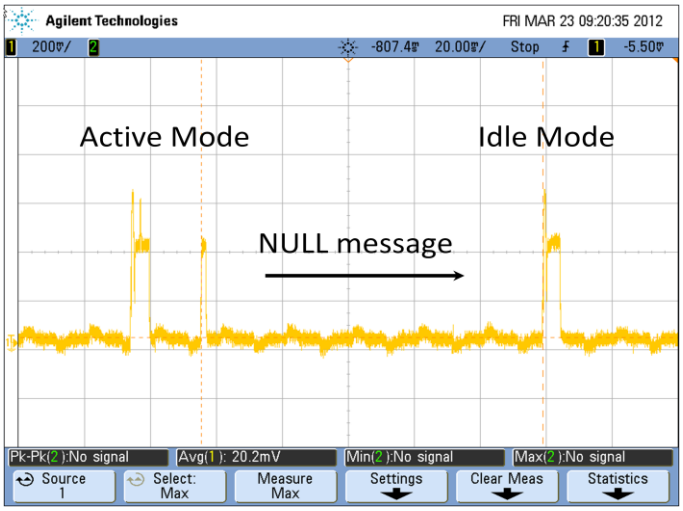


Figure 5-21 State transitions from active mode to idle mode

The flow control diagram for operations in active mode at the sensor node is shown in Figure 5-24. It starts from active mode of an individual node. The node can switch into the idle mode with two different approaches: 1) it can be forced into idle mode by user command messages; 2) automatic transition. For each channel period (time interval for a node to process one RF event), the node first examines the time period that the node has remained in idle mode, and compared it with a defined threshold value $T_{idle\_threshold}$, the node will automatically transition into idle mode if it has been idled for a certain period of time, otherwise the node will read a Rx messages buffer to confirm whether it has received an addressing message from the hub and whether it has a new event to report to the hub. Note that for a control unit such as joystick, it has to send back a data message during each designated channel period. Assume that an information message "1" is generated by the joystick and indicates that the wheelchair is driving forwards. It has to send this information to the hub immediately regardless whether or not it is the same as the previous one. However, for sensing nodes such as temperature or pressure sensor nodes, the wireless node has options not to send back any message while it receives an addressing message from the hub if the measurements do not change during the previous channel period. If the node determines not to send back any message, the host MCU will send a NULL message to the ANT transceiver and the ANT transceiver will not take any action while it reads a NULL message from the host MCU. And then it will add up the period of time it has been remains idle (T_{idle}) and return to the initial stage, waiting for the next addressing message from the hub. After it receives the messages from the hub, it will examine the message type, which could be an addressing message or a command message. The node will send a data message back if it receives an addressing message or the node will switch into different power modes if it is informed by the hub node with a command message. MSS

handshaking procedure will be performed prior to entering either parking mode or shipping mode.

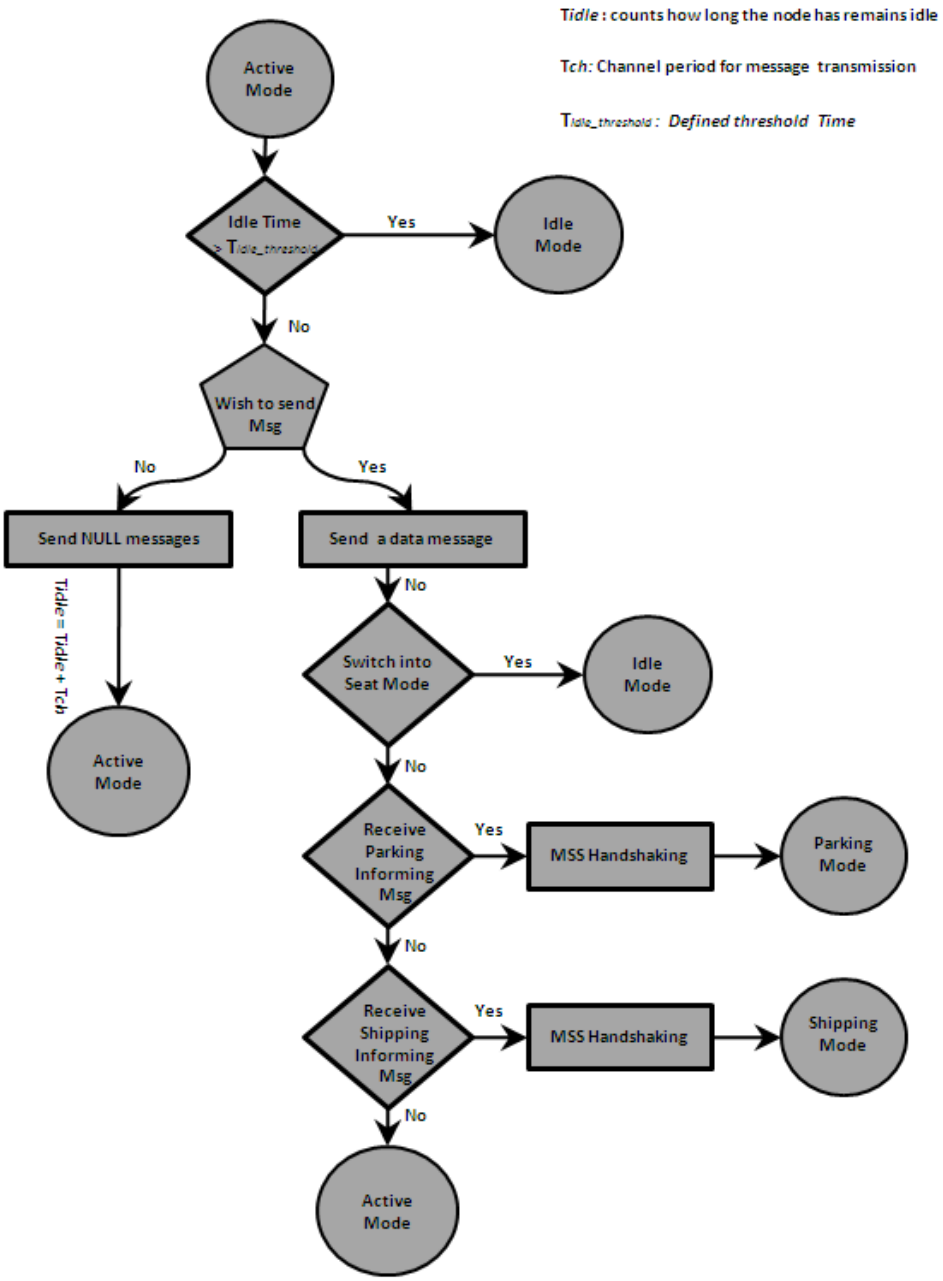


Figure 5-22 Flow control for operations in active mode.

While the wheelchair switches into seat mode for changing seat position, the distance sensor will enter into idle state for conserving power. In idle state, the distance sensor will still maintain the wireless link to the hub, receiving a heart beat message from the hub during each polling cycle without having to send data message to the hub. The operation of the distance senor in idle state is shown in Figure 5-23.

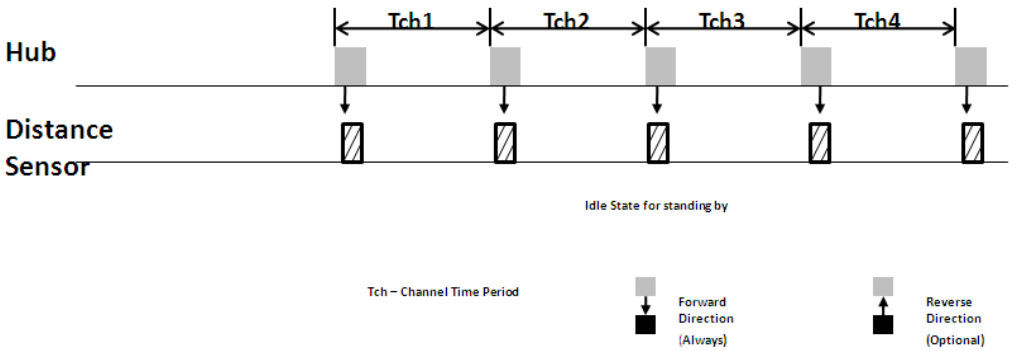


Figure 5-23 Operations of distance sensor in idle mode.

The flow control diagram for operations in idle mode is shown in Figure 5-24. It is shown that the control flow diagrams for operations in the idle mode is more straightforward, the remote node will send a null message during each channel period, and read the incoming message. It will only transition into other power modes if it has been informed by the hub node.

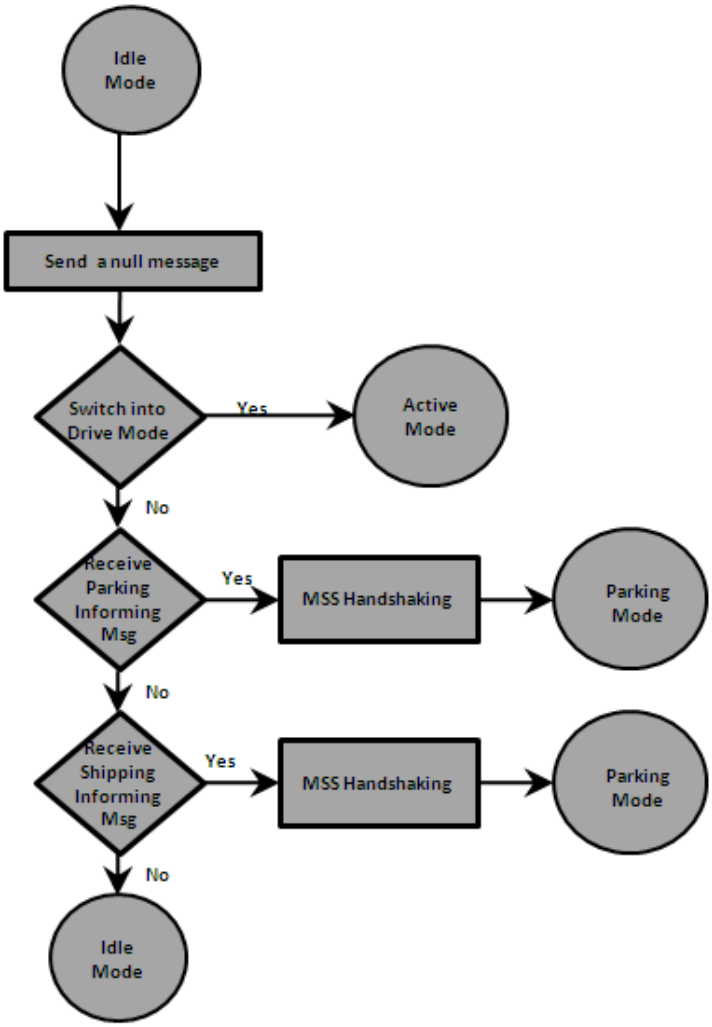


Figure 5-24 Flow diagram for operations in active mode.

If the wheelchair needs to be shut down overnight, the distance sensor node will enter into the parking mode (power down mode), and MSS will be performed to enable the network to operate in the continuous scanning mode. For operations in the continuous scanning mode, the communications are performed in an asynchronous fashion. Thus, the remote node can be configured to close all the channels to conserve power while it does not wish to communicate with the centre hub node and it can reopen a channel and rebuild the wireless link immediately at any time. This offers a great advantage for power conservation. In Figure 5-25, it shows that a remote node rebuilds a wireless link to the hub node from the status that all channels are closed and perform RF events immediately in the continuous scanning mode.

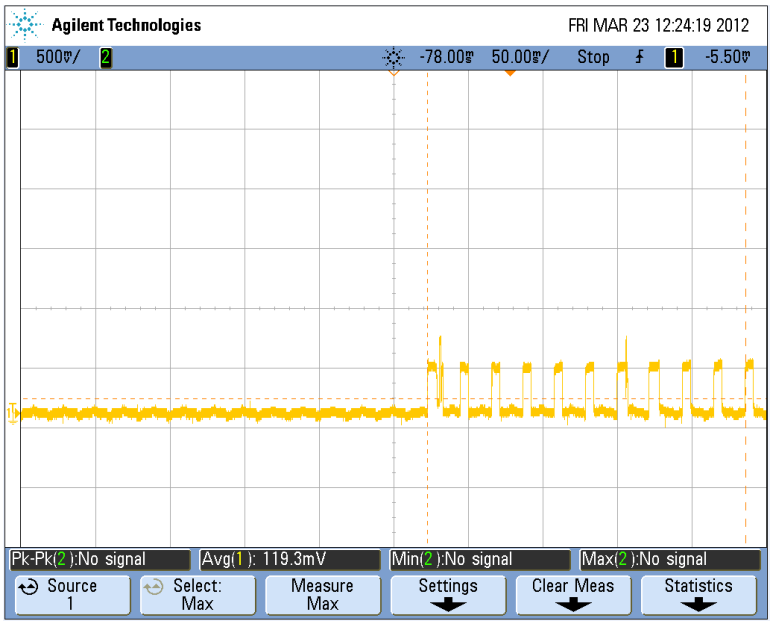


Figure 5-25 Remote node reopens a channel from the status that all channels have been closed

However, since it takes relatively long time to perform MSS, this methodology only suits the power modes in which the system can tolerate a long wakeup time, which are parking mode and shipping mode in this project. Figure 5-26 shows the procedure for transitions from the active mode into the parking mode. The remote node will perform handshaking protocol with the hub node to progress the MSS. The power performance is shown in the Figure 5-26. Note that the ANT transceiver will return two successive channel event messages to the host MCU in one channel period to confirm that a channel has been closed, as described previously in Figure 5-18.

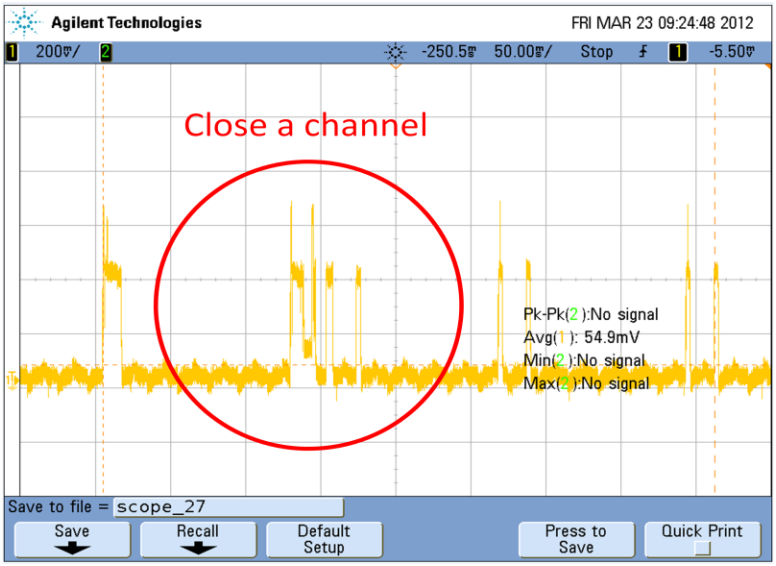


Figure 5-26 State transition from active mode to parking mode.

Since the system can tolerate up 10 seconds wakeup time. Thus, the distance sensor node will wake up every ten seconds for sending heart beat message to the hub node and close all the channels for the rest of the time, which is shown in Figure 5-27. The hub node will be active at full time.

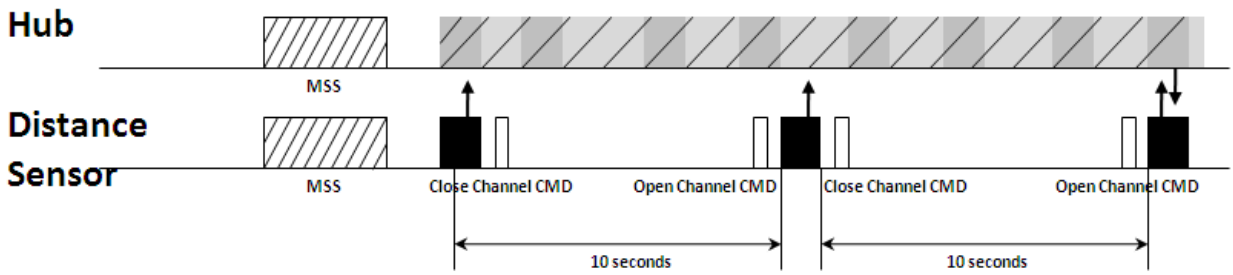


Figure 5-27 Operations of distance sensor in parking mode.

For operations in the parking mode, the parking mode may remain in this mode for a prolonged time period (up to several days or even longer). The hub node requires status information from the remote nodes for system monitoring purpose for the next wakeup. In this way, the system can perform system check prior to turning the system into active mode. Hence, the hub node requires the remote node to send heart beat message which contains diagnostic information. The diagnostic information indicates the status of each remote node which could be presence, absence or working improperly.

While running the node in the parking mode, the sensor node will periodically wake up and send heart beat message to the hub. During the period the remote node stands by and waits for the next transmission, the distance sensor node could be switched into either deep sleep state by sending a deep sleep command message or idle state by closing all the channels. If the remote node enters into deep sleep state, it consumes less power. However, all the channel

configurations will be erased. Thus, during each time the sensor node wakes up, all the channels have to be reconfigured before it can open the channel for RF activities. For operations in the parking mode, it means that the sensor node will have to reconfigure the channel every ten seconds. Channel configurations are implemented by sending serial messages between the host MCU and the ANT transceiver back and forth and it will consume a large amount of power, which can be illustrated in Figure 5-35 and discussed in Section 5.6. Reconfiguring the channel too frequently is not power-efficient. It is recommended to switch the sensor node into idle state to avoid frequent channel reconfiguration.

Note that the hub node only receives heart beat messages from the sensor node to confirm its status without sending messages in the reverse direction. However, if the hub node has accepted command message to wake the whole system up from the parking mode, it will send informing message back to the sensor node, which is shown in Figure 5-27. And the network will perform MSS, a set of handshaking procedure will be performed to reconfigure the hub node as a master device and all the remote nodes operate in the shared channel mode as slave devices.

The flow control diagram for operations in parking mode is shown in Figure 5-28. During each time period, the host MCU computes the time period that the node has remained in the idle state and compares it with a predefined threshold. The threshold is predefined by a certain number N_p. N_p represents the number of channel periods that the remote node takes to stay in the idle state:

$$N_p = Time\_Interval(Sec) \times Message\_Rate(Hz) \qquad (1)$$

For example, the time interval between two wakeups for a remote node is 10 seconds, and the message rate is 8 Hz. N_p can be computed by Equation 1, giving a result which is 80. Therefore, the remote node will remain in idle state for 80 channel periods, the host MCU will then wake up the ANT transceiver by opening channel 2 and broadcast a message to the hub node. Once channel 2 has been opened, the remote node will transmit a heartbeat message to the hub node to report its status, and the idle time will be set to 0. After the transmission has been completed, the remote node will close channel 2 immediately. When the hub node receives a user command to wake up the system, the hub node will keeping send a command message to the network by broadcast messages at a very high message rate. Once the remote node opens channel 2, it will receive the informing message and then switch into drive mode by implementing MSS handshaking procedure.

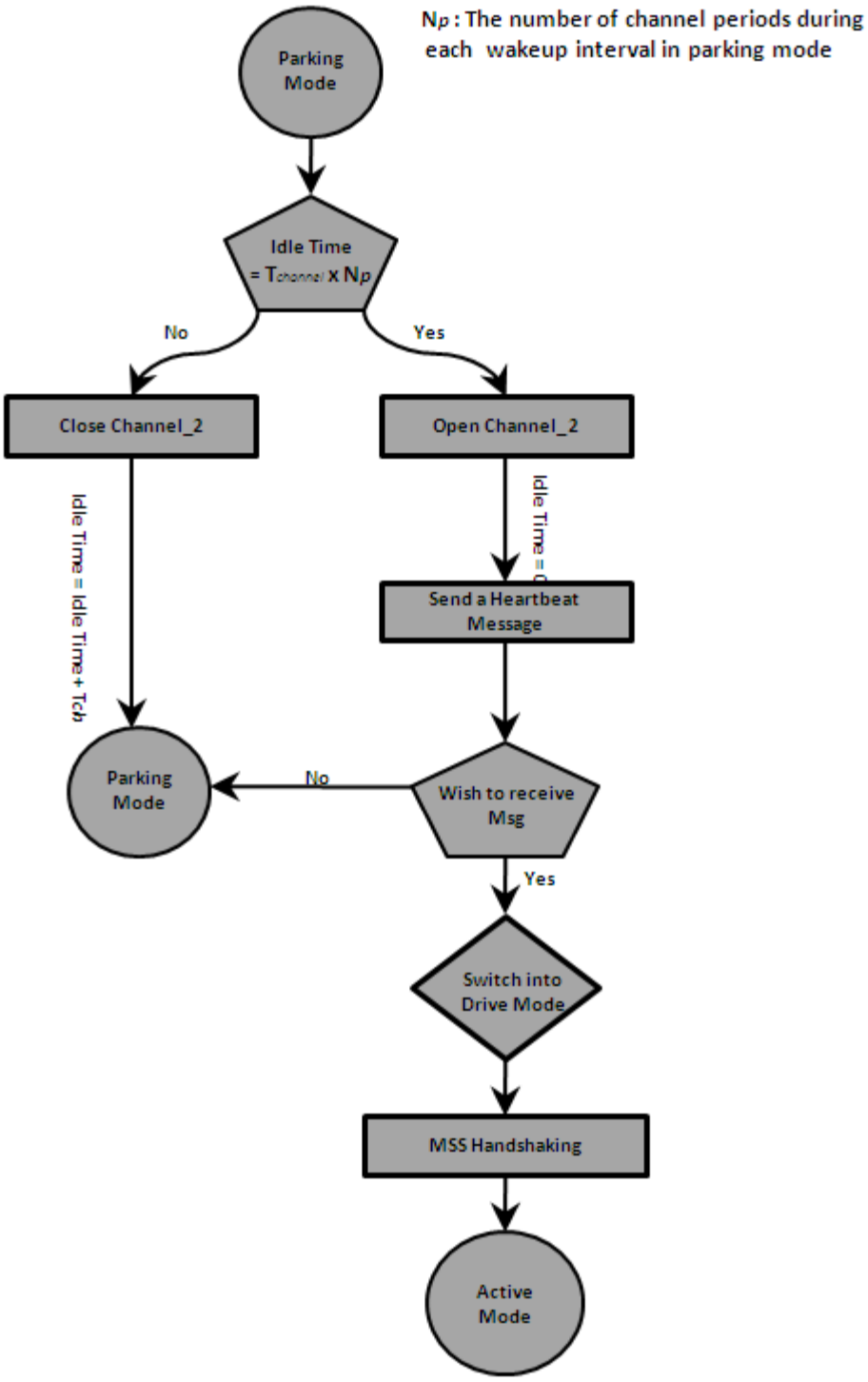


Figure 5-28 Flow control for operations in parking mode.

For operations in the shipping mode, the power management is similar to that in the parking mode. One major difference is that the system can tolerate up to two minutes wake up. Thus the time interval for sensor node wake up can be set to two minutes, as shown in Figure 5-29.

Thus, the sensor node can be switched into the deep sleep state, and configure the channel every two minutes to rebuild the wireless link.

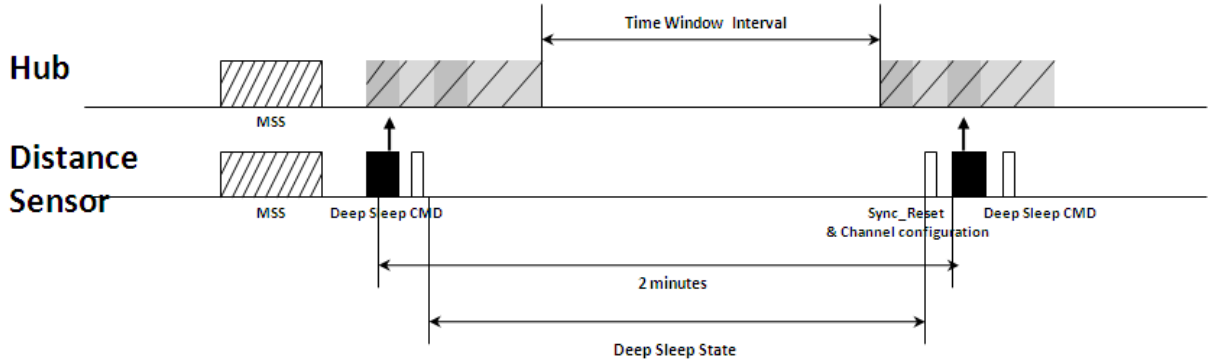


Figure 5-29 Operations of distance sensor in shipping mode.

On the other hand, shipping mode is designed for a power wheelchair to manage power while it is stored in the warehouse or transported to retailers, the wheelchair may operate in shipping mode up to several months without recharging power. The power consumption for the hub node to operate in the continuous scanning mode is 18 mini-amperes, which means the power consumption for maintaining the scanning channel may potentially run out of the battery. Thus, for operations in the shipping mode, the hub node will only open a time window for receiving heart beat messages periodically, and enters into idle state for the most of the time. This is illustrated in Figure 5-29 and the flow control diagram is shown in Figure 5-30.

In Figure 5-30, it shown that the flow control in the shipping mode is similar to that in the parking mode. One major difference is that the remote node enters into deep sleep mode once it completes a transmission. The current consumption is less in the deep sleep state compared with that in the idle state. However, the remote node has to do channel configuration each time it wakes up from the deep sleep mode. As the remote node wakes up for every 2 minutes in the shipping mode, the power conservation that the remote node benefits from switching into the deep sleep mode is larger than the energy cost for channel configuration.

The continuous scanning mode offers a great advantage for conserving power due to its asynchronous nature: it allows a remote node to close all the channels while it does not wish to communicate with the centre hub node, and rebuild the wireless link immediately once it opens a channel. However, it presents disadvantages for managing a large-size network which contains a large number of remote nodes. While operating in the continuous scanning mode, it presents a multi-master, single-slave infrastructure, thus the centre hub node is not able to offer precise timing control of channel management. Consequently, transmissions from multiple remote nodes may collide or overlap. A simple solution for that is to retransmit the message if communication collision or overlap is encountered. The retransmission rate is proportional to the message rate and the number of remote nodes. More studies are required to figure out the relationship mathematically. In this project, all prototyping is performed with a peer-to-peer scenario, thus, no study has been conducted with regard to communication collision and retransmission.

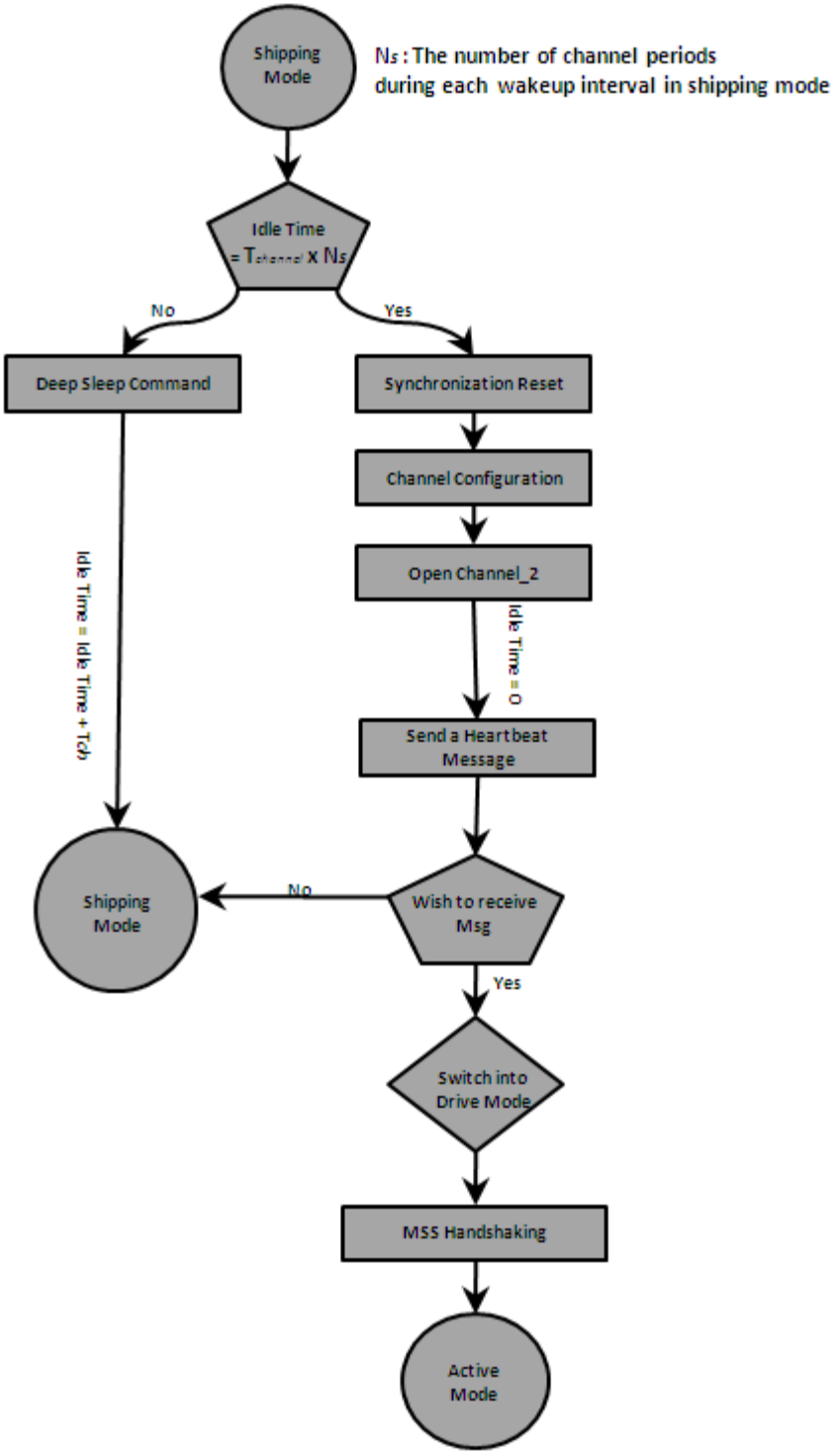


Figure 5-30 Flow control diagrams for operations in shipping mode.

In this section, a methodology has been introduce to develop a power management module to match the requirements of the power wheelchair based upon the power states and state transitions provided by ANT protocol. In this section, operations of remote and hub nodes in

different modes are illustrated with a case study. It only provides a basic power management module for future development in this section, and more research will be required for future work, including reliability, system control loop, hardware and etc.

Note that even the remote nodes operate in the continuous scanning mode, the triggering mode for them is still in the schedule driven mode. Since the continuous scanning mode only allows the remote nodes to send heart beat message without having to receive the addressing messages from the hub, however, the remote node will determine to transmit messages depending on the timeslot which has been allocated to it. The event-driven mode means that the remote node will only transmit messages to the hub whenever an event has been detected and keep idle otherwise. More details will be described in the following section.

For power consumption of host MCU, the host MCU will have to leave at least one timer running to manage scheduler operation. However, for each serial message transaction, the host MCU can be set to low power mode once the transaction has been completed, and wakeup prior to processing the next message transaction. In this project, the selected MCU is the chipset from MSP430 family. It offers a fast and straightforward fashion offers able to switch the power states. This can be interpreted by the pseudo codes below:

```
 PowerMode_BIT = 0;              // Wake up MCU from low power mode
Main_ProcessANTEvent ();         // Process serial interface message
PowerMode_BIT = LPM4_bit;        // Initialize the low power mode to mode 4
_BIS_SR (PowerMode_BIT);         // MCU enters low power mode 4
```

The power consumption of host MCU is not the focus in this thesis, however, it is essential to take insight into it for estimating node lifetime. More details can be found in data sheet of MSP430 [96].

5.5 Node Lifetime Estimator

To accomplish the motion detection on a power wheelchair, two approaches are discussed in this thesis: event-driven and schedule-driven. In event-driven operation, a sensor filters the incoming data and determines to wake up and transmit a data message if it is different from the previous one. In schedule-driven operation, the sensor nodes are connected directly to the main processing unit. The processor follows a pre-configured schedule and alternates the system between a low-power and active (full-power) mode to conserve the power. The network structure for both modes is shown in Figure 5-16.

With event-driven mode, the remote sensor nodes are configured as master nodes so that they have autonomy to send messages. This is because, with the ANT protocol, slave nodes can

only transmit messages while they receive the polling message from the master nodes in the shared channel mode.

The operation of the system is simplified into four modes which are listed in Table 12. Some impractical modes are eliminated. For operations in the continuous scanning mode, the remote node is configured to close all the channels while it does not wish to send any message to the hub node. While for operations in the shared channel mode, the remote node will continuously listen to the channel to maintain the channel synchronization.

Operation Mode / Power Mode	Continuous scanning mode		Shared channel mode	
	ANT transceiver	Host MCU	ANT transceiver	Host MCU
S_1(Idle)	Idle	LPM4	N/A	N/A
S_2(Processing)	Idle	Active	sleep	Active
S_3(Tx)	Tx	Active	Tx	Active
S_4(Rx)	Rx	Active	Rx	Active

Table 12 Power states.

For operations in the continuous scanning mode, a remote node always starts an operation from the idle state S_1, in which the remote node is configured to close all the channels and the host MCU remains in a low power mode (LPM4), only a sensing unit is operating to collect data from environment. In the processing state S_2, the host MCU reads the collected data and compares it with the previous one to determine whether to send it or not. If the data message is the same as the previous data, the system returns to the idle state, otherwise it will transition into Tx state S_3 by opening an active channel and building a wireless link with the hub node. And then the node will listens to the channel in Rx state S_4 for receiving an acknowledgement message from the hub to confirm that the data message has been successfully transmitted. If not, the remote will return to S_3 and retransmit the previous data message.

While the network operates in the shared address mode, it is more straightforward to model the flow control: a remote node has to listen to the channel during each channel period, and it will not send a data message to the hub if the collected data remains the same during the previous channel period. As for the operations in the shared address mode, the hub node

controls the timing of each shared channel, transmission collision or overlap will not occur for each remote node in its designated channel period, the node will not have to listen to the channel after it sends a data message to the hub. Instead, it will return to S_3 directly.

The mathematical model is built on the assumptions listed below:

1. Events arrivals follow a Poisson distribution.
2. Processing and radio-transmission times are independent and identically distributed (i.i.d) with arbitrary distribution.
3. Radio transmission in a noise-free environment, the transmission will only fail due to channel collision.
4. When an event is detected, if it is the same as the previous one, the node will not send any data message. The node processes it and sends the information to a hub node with probability α.
5. Assume an ideal environment, in which the remote node will not retransmit messages due to the interference or noise.
6. After a message is sent, the probability of retransmission is ρ, which is proportional to the size of the network and the duration of channel periods.

Start with a simple model with the following assumptions:

1. Only peer-to-peer communication applied
2. Only remote node is modeled, while the base station is powered by a main battery and the power source is assumed as infinity
3. The transmission type is set as broadcast, so that retransmission is not taken account into the model.

The power state transition for event-driven mode during wakeup period is shown in Figure 5-31.

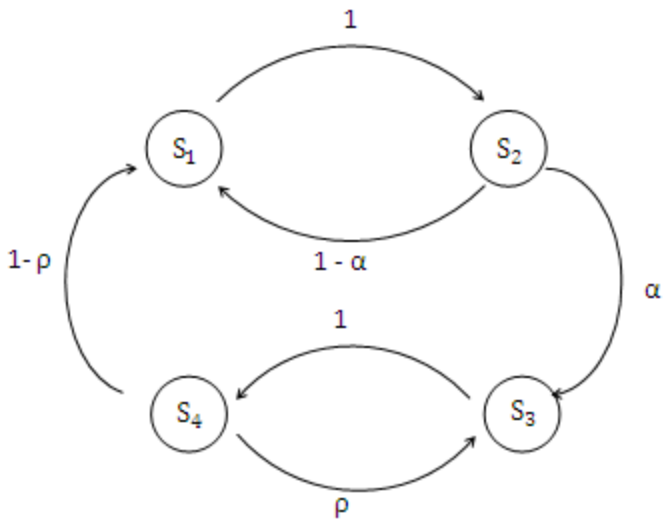


Figure 5-31 Power state transition with event-driven mode.

In this mode, S_1 is the monitoring stage, once a sensor continuously sample the environment data, it will trigger the message transmissions immediately when an object enters the vicinity of the wheelchair. Then the remote nodes listen to the acknowledge message from the hub node to determine whether or not to retransmit the messages.

Given the total amount of energy per node E_{Total}, the lifetime can be approximated by the equation:

$$\sum_1^4 E_{S_k} + E_{S_{12}} + E_{S_{23}+}E_{S_{34}} + E_{S_{41}} \leq E_{Total} \qquad (2)$$

The basic idea is to compute long-run proportion of transitions into state i. Let p_i denote the steady state probability of mode i, during a long enough time period T, the total time spent at state i can be approximated as $\lim_{T\to\infty} T_i = T \times p_i$. Therefore, the total energy spent at state i is $E_{S_i} = Tp_i \times P_{S_i}$, for i $\in \{1,2,3,4\}$, where P_{S_i}denotes the power consumption at state i. And the transition energy cost from state i to j during T can be obtained as $E_{S_{ij}} = C_{ij}\bar{n}_{ij}(T)$. C_{ij} denotes the energy cost during the transition from mode i to j and $\bar{n}_{ij}(T)$ is the total number of transitions occurred during time period T. Let π_i denotes the proportion of transitions into the state i, and μ_i denotes the average time spent in state i before making a transition, then the steady state probability of state i, p_i can be computed by

$$p_i = \frac{\pi_i \mu_i}{\sum_j \pi_j \mu_j} \qquad (3)$$

π_i can be solved by

$$\pi_{i=} \sum_j \pi_j p_{ji}, \ \sum_i \pi_i = 1 \qquad (4)$$

Then, by applying (2), the following equations are obtained:

$$\sum_i \pi_i = 1\,, i \in \{1,2,3,4\};\ \overline{\pi}\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1-\alpha & 0 & \alpha & 0 \\ 0 & 0 & 0 & 1 \\ 1-\rho & 0 & \rho & 0 \end{pmatrix} = \overline{\pi}\,,\ \overline{\pi} = (\pi_1\ \pi_2\ \pi_3\ \pi_4)\ (5)$$

The solution gives $\pi_1 = \pi_2 = \frac{1-\rho}{2(1-\rho)+2\alpha}$ and $\pi_3 = \pi_4 = \frac{\alpha}{2(1-\rho)+2\alpha}$, therefore, the steady state probability of each state can be computed:

$$p_1 = \frac{(1-\rho)\overline{X}}{D(\alpha)}, p_2 = \frac{(1-\rho)\overline{Y}}{D(\alpha)}, p_3 = \frac{\alpha\overline{Z}}{D(\alpha)}, p_4 = \frac{\alpha\overline{L}}{D(\alpha)}$$

Where $\overline{X}$, $\overline{Y}$, $\overline{Z}$ and $\overline{L}$ are the average process time of each state and $D(\alpha) = (1-\rho)\overline{X} + (1-\rho)\overline{Y} + \alpha\overline{Z} + \alpha\overline{L}$. Therefore, the total energy cost E_{S_i} at state i can be approximated by:

$$E_{S_1} = \frac{T\overline{(1-\rho)\overline{X}}P_{S_4}}{D(\alpha)},\ E_{S_2} = \frac{T(1-\rho)\overline{Y}P_{S_2}}{D(\alpha)},\ E_{S_3} = \frac{T\alpha\overline{Z}P_{S_3}}{D(\alpha)}, E_{S_4} = \frac{T\alpha\overline{L}P_{S_4}}{D(\alpha)}$$

And the event arrivals follow a Poisson distribution with average inter-arrival rate λ, we can approximate the steady state probability by:

$$p_1 = \frac{1-\rho}{(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})}, p_2 = \frac{\lambda(1-\rho)\overline{Y}}{(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})},$$

$$p_3 = \frac{\lambda\alpha\overline{Z}}{(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})}, p_4 = \frac{\lambda\alpha\overline{L}}{(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})}$$

Thus, node lifetime is given by:

$$T_L(\lambda) = \frac{[(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})]E_{Total}}{(1-\rho)P_{S_1}+\lambda[(1-\rho)\overline{Y}\overline{P}_2+\alpha\overline{Z}P_{S_3}+\alpha\overline{L}P_{S_4}+C_D]} \qquad (6)$$

Where C_D is the total power cost per event of transition state. The major power cost for state transitions occurs while opening or closing a channel which are $E_{S_{23}}, E_{S_{41}}$. Thus equation (5) can be simplified as:

$$T_L(\lambda) = \frac{[(1-\rho)+\lambda[(1-\rho)\overline{Y}+\alpha\overline{Z}+\alpha\overline{L})]E_{Total}}{(1-\rho)P_{S_1}+\lambda[(1-\rho)\overline{Y}\overline{P}_{S_2}+\alpha\overline{Z}P_{S_3}+\alpha\overline{L}P_{S_4}+\ C_D]} \qquad (7)$$

The power transition diagram of schedule-driven mode is shown in Figure 5-32. In this scheme, remote sensor nodes are configured as slave nodes, the hub node is the master node which polls all the remote slave nodes within the network during each cycle and asks for data messages from the remote sensors. In this scheme, the remote sensor node keeps listening to

the channel in each polling cycle to receive the addressing messages from the hub. It will transmit a data message back with a probability α.

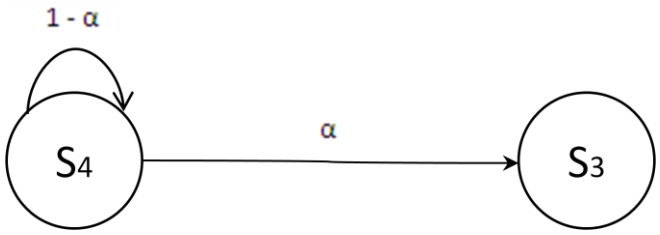


Figure 5-32 Power transition with schedule-driven mode.

The modeling strategy of schedule-driven model is different from the event-driven model. The basic idea is to compute the average power consumption during each channel period. During each channel period, the remote node will receive one addressing message, and transmit back a data message with probability α. For the rest of time, the ANT transceiver will remain in sleep state, in which the channel remains open, but no RF event is performed.

Let $\overline{C}$ denotes the process time for one channel period, during each channel period, the average power consumption is:

$$P_{Average} = \frac{\left[\overline{C} - \overline{\alpha Z} - \overline{L}\right)\overline{P}_{S_2} + \alpha\overline{Z}P_{S_3} + \overline{L}P_{S_4}}{\overline{C}} \qquad (8)$$

The average node lifetime can be obtained as:

$$T_L = \frac{E_{Total}}{P_{Average}} = \frac{E_{Total}\overline{C}}{\left[\overline{C} - \overline{\alpha Z} - \overline{L}\right)\overline{P}_{S_2} + \alpha\overline{Z}P_{S_3} + \overline{L}P_{S_4}} \qquad (9)$$

As shown in the equation (7), the power lifetime for event-driven mode is majorly determined by the event inter-arrival rate λ and the probability of retransmission rate ρ, while for schedule-driven mode, the node lifetime is determined by the channel period $\overline{C}$.

5.6 Measurements

For evaluating the power consumption of the wireless platform, since the supply voltage is kept constant, the power consumption can be measured by the current drawn. Thus, the current can be measured through measuring the voltage drop across a shut resistor connected in series with the power supply of the transceiver drop-in module. An oscilloscope is used to take measurements of voltage drop across the shut resistor, and therefore obtain the current across it. The experiment setup is shown in Figure 5-33 and Figure 5-34.

The measurements are taken while implementing a peer-to-peer wireless communication between a master hub node and a slave remote node. A 100Ω shunt resistor is connected in series with the power supply pin of the remote node prototype since the power consumption on the remote end is the focus in this project. An USB port JTAG programmer is used for programming and debugging purpose in the measurements.

The shunt resistor is connected to the power supply pin of the ANT transceiver drop-in module to eliminate the impact of host MCU and other peripheral hardware devices on the measurements of the ANT transceiver. All the LEDs are disabled before taking the measurements.

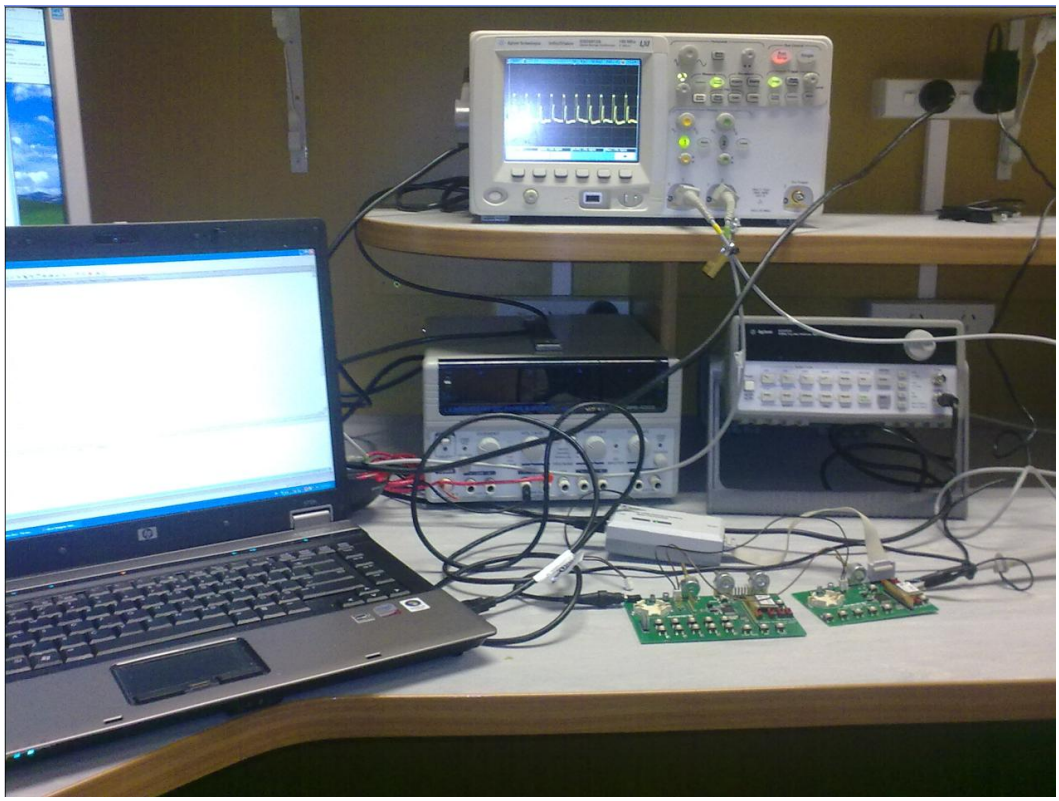


Figure 5-33 Laboratory setup.

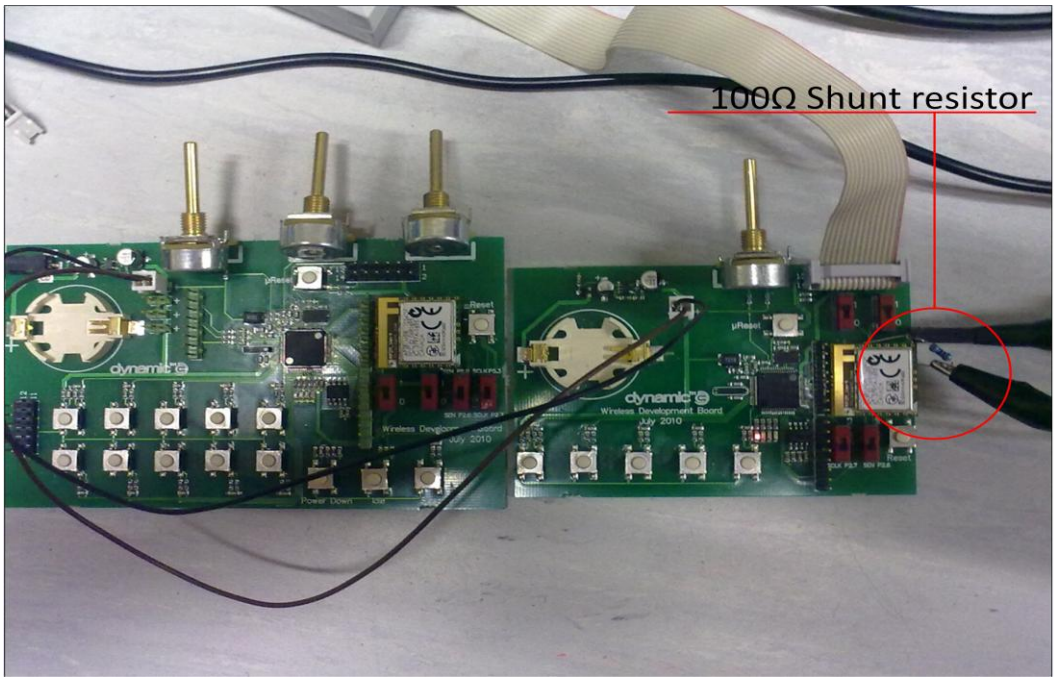


Figure 5-34 Shunt resistor setup

ANT channel is configured with default transmission power level of 0 dBm and message rate of 8 Hz (125 mini-seconds channel period). Figure 5-35 shows the current drawn during the channel configuration procedure. During channel configuration, the host MCU sends configuration commands to define each field with appropriate parameters, and all configuration commands will return a channel event message to indicate the success or failure. In Figure 5-35, it shows that the host MCU sends configuration commands every 10 mini-seconds followed by a response message, the signal pattern on the oscilloscope indicates that the host MCU continuously sends the configuration messages and receives the channel event messages. The peak value of the voltage across the shunt resistor is 612 mini-volts, indicating that the peak current drawn is approximately 6.12 mini-amperes. The average current drawn in this procedure is approximately 2 mini-amperes with a 100 Hz message rate. For processing each configuration field, one command message is sent to the ANT transceiver via serial interface and it takes approximately 2.4 mini-seconds to process.

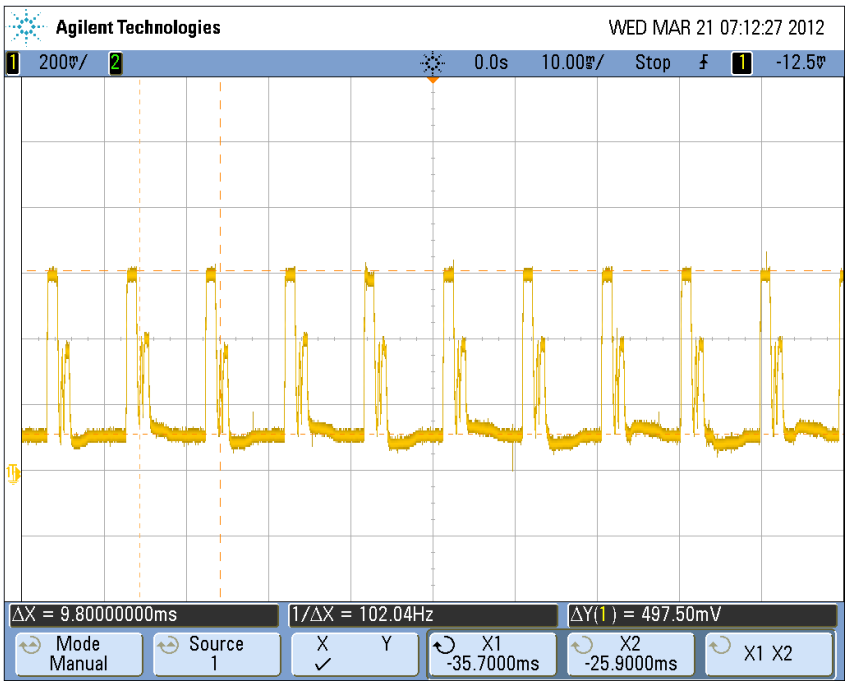


Figure 5-35 Instant current consumption for channel configuration.

The remote node enters into active mode while the channel configuration procedure completes, the voltage pattern across the shunt resistor is shown in Figure 5-36. In active mode, in each channel period, the remote node receives an addressing message from the hub node and then transmits a data message in the reverse direction. As shown in Figure 5-36, the average current consumption for such a procedure is approximately 4.3 mini-amperes, and the duty cycle is approximately 7.8% (9.8 mini-seconds out of one channel period which is 125 mini-seconds). The average current drawn varies from 360 micro-amperes to 400 micro-amperes during a long run measurement and the typical value is around 380 micro-amperes. The result is shown in Figure 5-37. The voltage pattern presents two impulses in each channel period, indicating that the ANT transceiver instantaneously draws a large amount of power to implement RF message reception and transmission in a short time. Since the remote node always receives an addressing message first and then transmits a data message back, the first impulse is generated while message reception and the second one correspond to message transmission. Note that the signal pattern comprises three portions. The first portion is the RF message reception and transmission. The second is serial interface message for communications between ANT transceiver and the host MCU. The third is the event message generated by the ANT node which indicates the channel status. This is illustrated by inserting a time delay following each RF reception or transmission, as shown in Figure 5-38.

Figure 5-36 Instant current consumption in active mode.

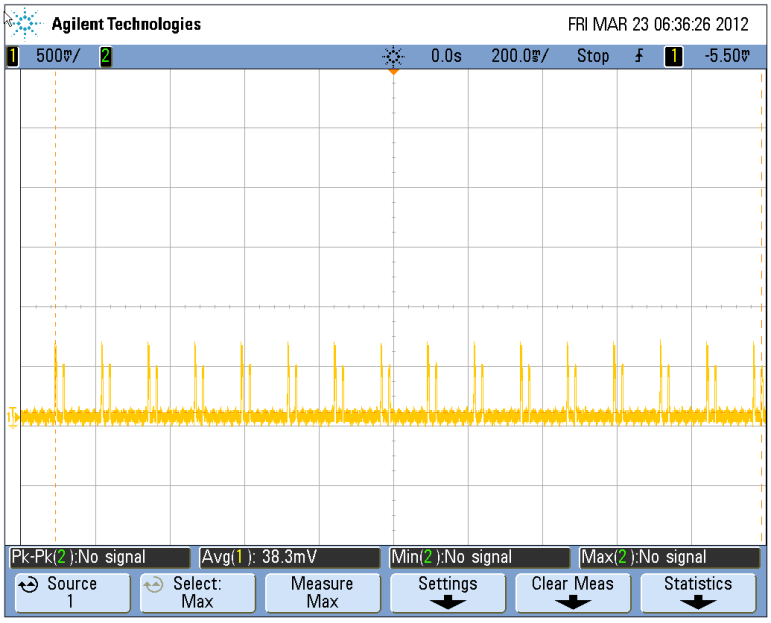


Figure 5-37 Long-run measurements in active mode.

In Figure 5-38, a time delay is inserted between RF messages (reception and transmission) and channel event messages. It shows that the channel event message consumes approximately 4 mini-amperes with duty cycle of 3.2% (4 mini-seconds out of 125 mini-seconds). This contributes a significant current consumption for implementing ANT node, but has not been described in ANT specification data sheet [92]. Channel event message is a 5-byte message with a fixed format, the last byte of the message is defined as message code to indicate the

channel status or success or failure of RF events. More details can be found in ANT protocol manual [100].

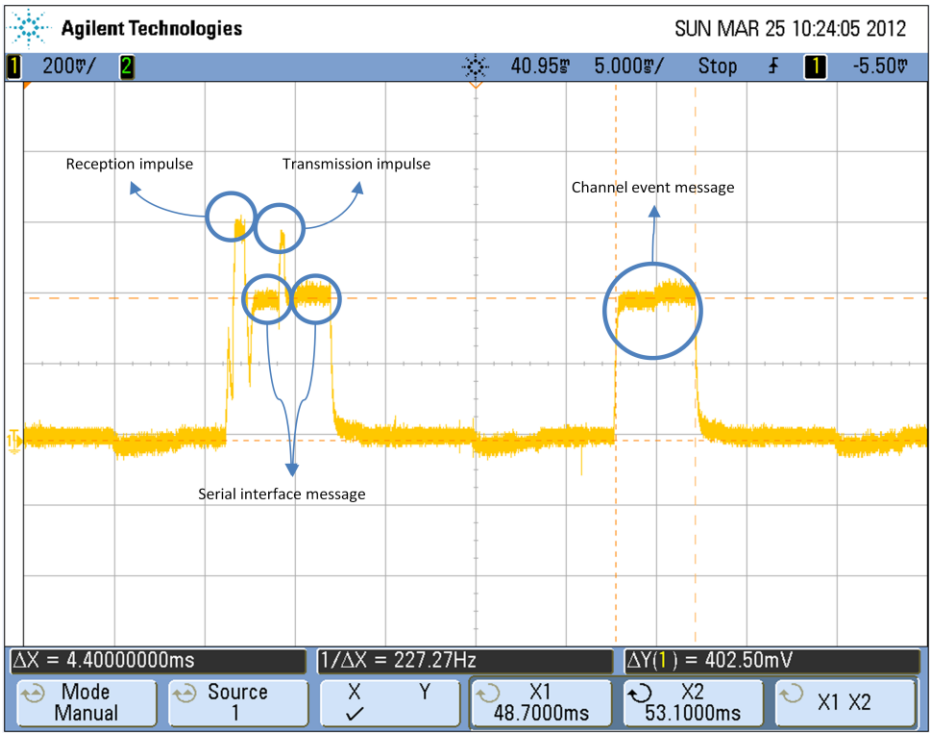


Figure 5-38 Composition of signal pattern.

To investigate the impact of settings of Tx power level on the current consumption, we set the Tx power level to -20 dBm and run the measurements. The measurement result is shown in Figure 5-40. Comparing Figure 5-39 with Figure 5-40, the results show that the setting of Tx power level has only slight impact on the total power consumption. Only the second impulse (message transmission) decreases slightly (from 6.4 mini-amperes to 6.1 mni-amperes) while -20 dBm Tx power is applied. Other portions of the voltage pattern still remain the same. The average current consumption is almost the same as the message transmission is operated with 0 dBm Tx power level.

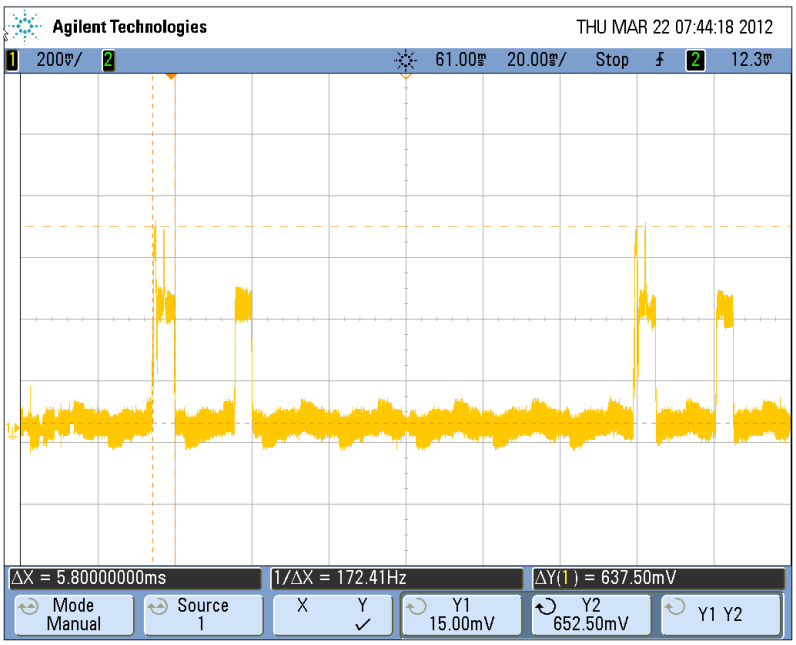


Figure 5-39 Measurements with 0 dBm Tx power level.

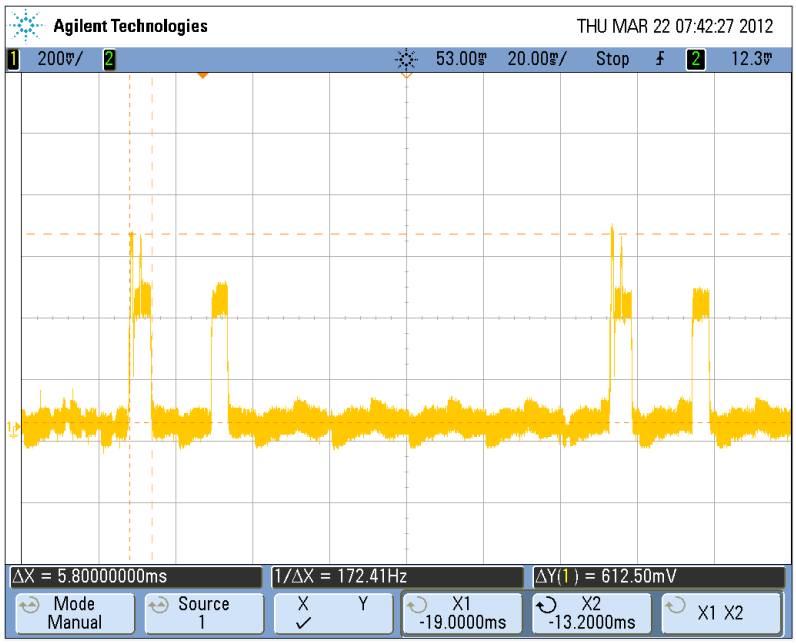


Figure 5-40 Measurements with -20 dBm Tx power level.

Then the remote node is switched into idle mode, in which the node listens to the channel for receiving the messages only. As shown in Figure 5-41, the duty cycle for message reception is approximately 3.84% (4.8 mini-seconds out of 125 mini-seconds), note that there is no event message returned for message reception. The average power measurement across the shunt resistor during a long-run varies from 20 mini-volts to 23 mini-volts, and the typical value is

around 22 mini-volts. The result is shown in Figure 5-42. Note that there is no channel event message for message reception.

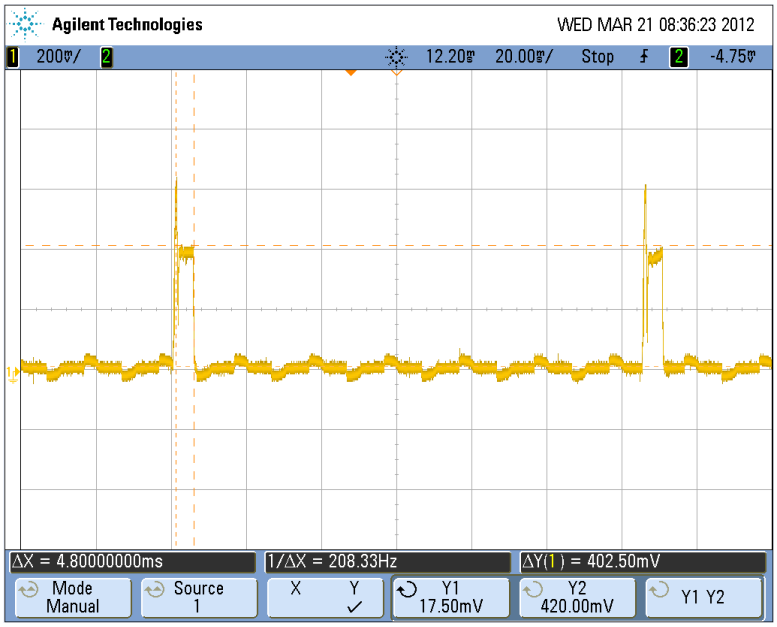


Figure 5-41 Instant current consumption in idle mode.

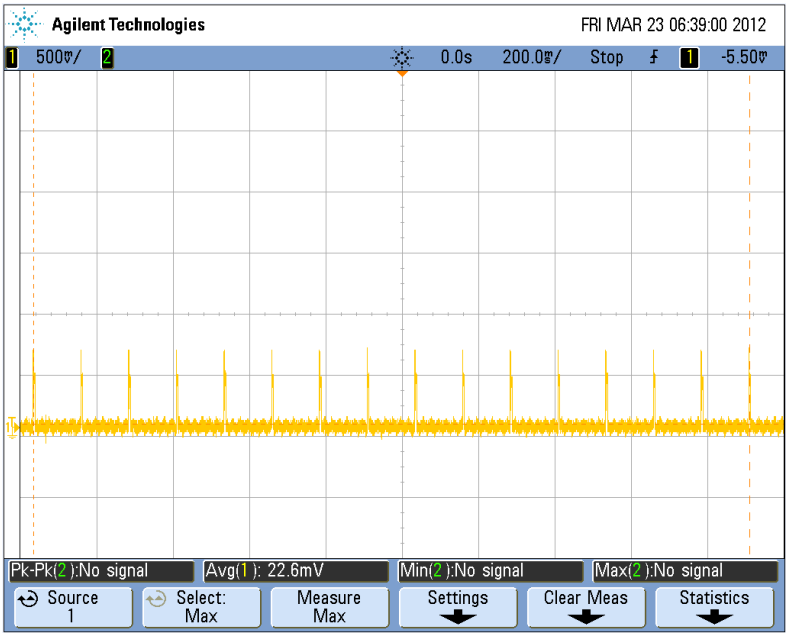


Figure 5-42 Long-run measurements in idle mode.

By implementing MSS handshaking procedure, the remote node is re-configured as a master node, and transmit message to the centre scanning node (the hub node) only. The signal pattern is shown in Figure 5-43. The duty cycle for message transmission is relatively small, only

2.24% (2.8 mini-seconds out of 125 mini-seconds), the peak value of impulse response is 660 mini-volts. The duty cycle of channel event message is about 2.56% (3.2 mini-seconds out of 125 mini-seconds). The result of long-run measurements shows that the average current consumption varies from 210 micro-amperes to 240 micro-amperes and the typical value is approximately 230 micro-amperes, as shown in Figure 5-44.

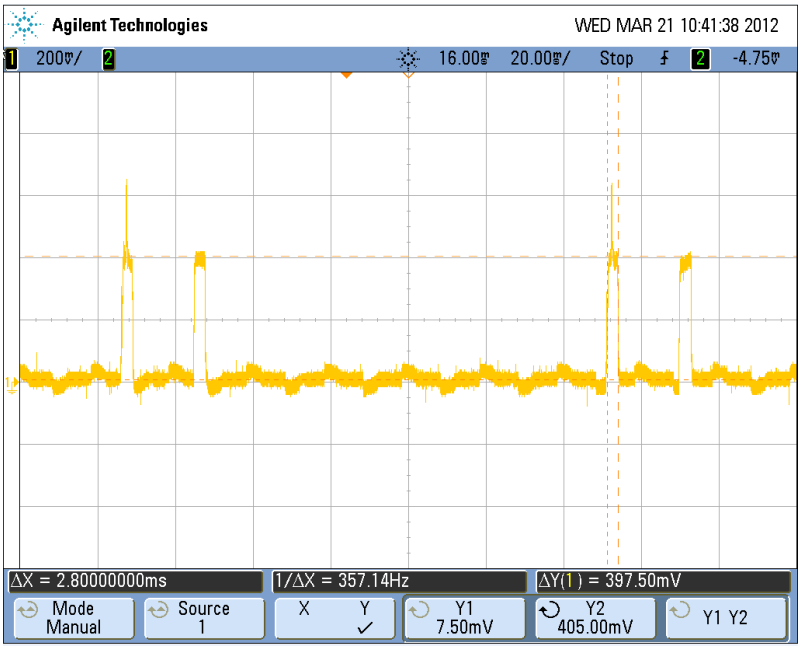


Figure 5-43 Instant current consumption in the scanning mode.

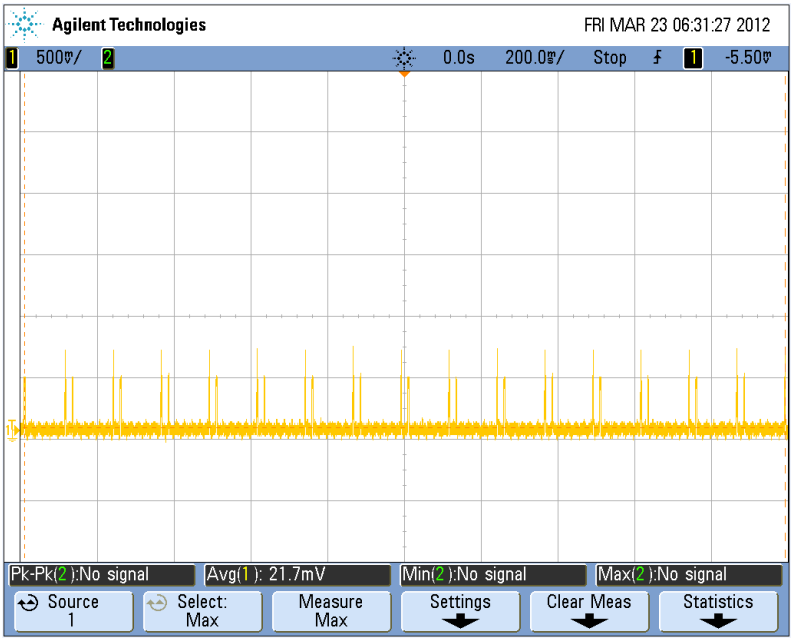


Figure 5-44 Long-run measurements in the scanning mode.

For the central scanning node, the average current is approximately 6 mini-amperes, as shown in Figure 5-45, which differs from the value (~18 mini-amperes) presented in protocol user manual [93].

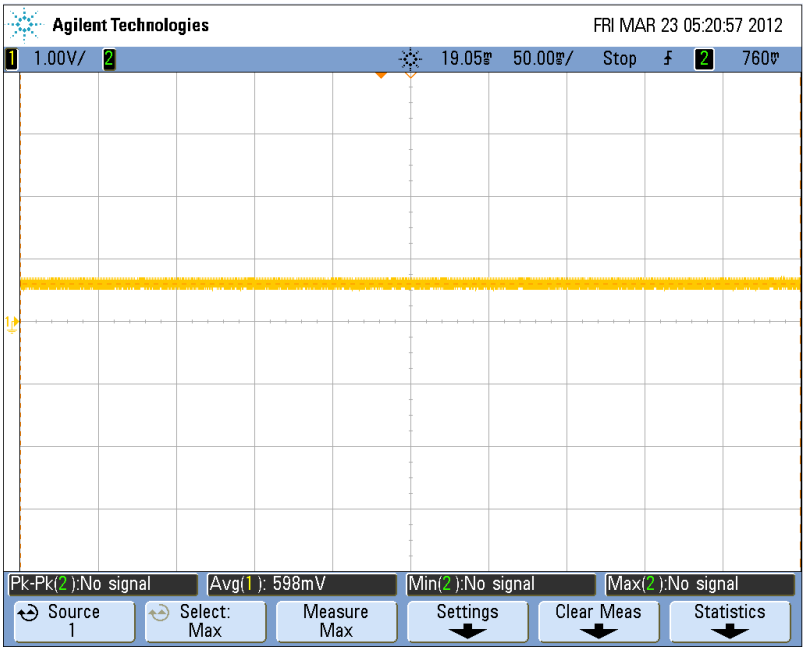


Figure 5-45 Average current consumption on the scanning node.

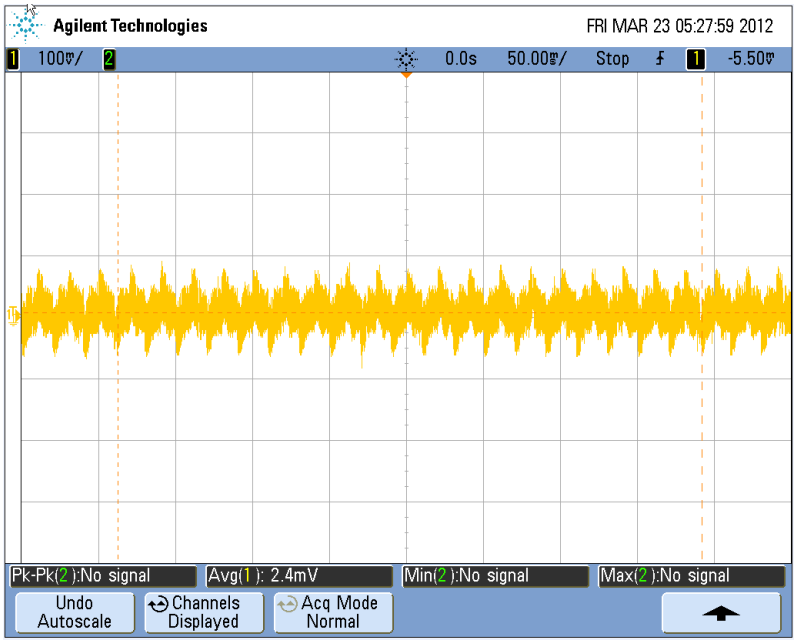


Figure 5-46 Average current consumption while all channels are closed.

While all channels are closed, the measurements present a large variation (from -2.6 mini-volts to 13.5 mini-volts) due to the increased signal-to-noise ratio (SNR). It is difficult to obtain

precise measurements with an oscilloscope. An instant observation is shown in Figure 5-46. For node lifetime estimation, we will apply the values provided in ANT specification data sheet, as shown in Table 9.

The measurements laboratory can be summarized as:

1. The variation of the measurements is relatively large, for more precise measurements, a LabView program is required to communicate with the wireless node through a GPIB link to take samples in its internal memory and obtain an average value of the current consumption and time period of RF reception and transmission during a long run.
2. For measuring the current consumption while the ANT node operates in low power state (e.g. sleep, idle or deep sleep state), it is required to eliminate the noise interference. In this laboratory, the precise results of current consumption in low power states cannot be obtained due to the constraints of equipment and methodology.
3. This laboratory is designed for measuring the current consumption on ANT transceiver. For the whole system, the current consumption of host MCU, sensors, power regulator and other peripheral device are required to estimate the node lifetime.
4. The measurement of current consumption in the central scanning mode in the continuous scanning node greatly differ the value presented in the specification data sheet.

The obtained results differ from the specifications presented in ANT specification data sheet. This may be caused by:

1. The measurements are taken from an on-board ANT transceiver, thus it does not completely eliminate the impact of activities of host MCU and other peripheral devices on the ANT transceiver, which will increase the values of measurement.
2. The prototype for measurements employs a drop-in module instead of chip-based solution. The drop-in module offers a complete RF circuitry and antenna, and a protocol engine is embedded to offer ease of development. However, the current consumption is larger compared with ANT chip.
3. The specification table on the data sheet only summarizes the current consumption of transmission and reception. However, to successfully complete an RF event, a series of serial interface communications and channel event messages will contribute the current consumption as well. This is not described in details in the specification table.

The results of the measurements are summarized in Table 13.

Symbol	Power mode	Min	Typical	Max	Unit
I_{idle}	Rx-only in idle mode	200	220	230	µA
$I_{parking}$	Tx-only in parking mode	210	230	240	µA
I_{active}	Active mode	360	380	400	µA

Table 13 Measurements of average current consumption.

Note that the results are only valid for channel configuration with 8 Hz message rate and 0 dBm Tx power. In Table 14 and Table 15, it shows the timing and current measurements for ANT transceiver.

Symbol	Description	Min	Typical	Max	Unit
t_{Rx}	RF reception impulse processing time		580		µs
t_{Tx}	RF transmission impulse processing time		230		µs
t_{open}	processing time of Channel event message for ***Open_Channel*** command message	5.4	5.5		ms
t_{close}	processing time of channel event message for ***Close_Channel*** command message		8.2		ms
$t_{Tx\_completed}$	Processing time of channel event message for ***Transmit_Message*** command message		2.7		ms
t_{cmd_msg}	Processing time of command message which is sent to inform ANT transceiver to take corresponding actions		2.4		ms

Table 14 RF events timing

Symbol	Description	Min	Typical	Max	Unit
I_{Rx}	Average current of RF reception impulse	5.72	5.95	6.17	mA
I_{Tx}	Average current of RF transmission impulse	5.65	5.67	5.87	mA
I_{open}	Average current of Channel event message for ***Open_Channel*** command message		4.02		mA
I_{close}	Average current of Channel event message for ***Close_Channel*** command message		4.02		mA
$I_{tx\_completed}$	Average current of Channel event message for ***Transmit_Message*** command message		4.02		mA
I_{cmd_msg}	Average current of Command message which is sent to inform ANT transceiver to take corresponding actions		4.25		mA

Table 15 RF events current measurements

Note that the values of average current for different command messages are always the same. However, the average processing time of different command messages varies as they have different message length. Here, all the command messages are assumed to be the same in terms of both processing time and average current consumption for simplifying the estimation as the variation will not make a significant impact on the estimation.

With obtained results of current consumption and a mathematical model, the developers are able to estimate the node lifetime.

Scenario 1 is made based on the following assumptions:

1. The remote node is configured with 8 Hz message rate and 0 dBm Tx power;
2. Four remote nodes are deployed in the network, which means each remote node will transmit back to the hub for every four channel periods;
3. The daily usage for each remote node is 6-hour operations in the active mode, 6 hours in the idle mode and 12 hours in the parking mode;
4. To simplify the model, assume that the remote node will transmit data message in each designated cycle without considering the probability α for data transmission;
5. The remote nodes operate in the shared channel mode in active mode;
6. The remote node is powered by two CR2032 coin cell batteries, which provide a capacity of 400 mAh in total.

Here, as the message rate is 8 Hz and the Tx power level is set to 0 dBm, the measurements obtained in Table 13 can be applied directly to compute the average power consumption during the active mode can be computed by:

$$I_{active\_average} = \frac{3 \times I_{idle} + I_{active}}{4} = 260\ \mu A$$

For operations in the parking mode, the remote node wakes up every ten seconds to report the device status to the hub node, during this period of time, the node opens a channel for message transmission, and then it will close the channel. This whole procedure consists of seven successive events: 1) Open_Channel command message; 2) channel event message to confirm that the channel has been opened; 3) command message requests ANT transceiver to transmit; 4) data message transmission; 5) channel event message for message transmission; 6) Close_Channel command message; 7) channel event message for Close_Channel command message. The average current consumption is:

$$\begin{aligned} & I_{parking\_average} \\ &= \frac{I_{open}t_{open} + I_{close}t_{close} + I_{Tx}t_{Tx} + t_{tx\_completed}I_{tx\_completed} + 3t_{cmd\_msg}I_{cmd\_mesg}}{10 \times 10^3} \\ &= \frac{4020 \times 5.5 + 4020 \times 8.2 + 4020 \times 2.7 + 5670 \times 0.23 + 3 \times 4250 \times 2.4}{10 \times 10^3} \\ &= \frac{65928 + 1304 + 30600}{10 \times 10^3} = 9.78 \mu A \end{aligned}$$

The average current consumption in the idle state in which all channels have been closed is obtained from the data sheet ($2\ \mu A$). Thus the average current consumption is approximately 11.78 μA.

The node lifetime can be estimated by:

$$\frac{400 \times 10^3}{11.78 \times 12 + 260 \times 6 + 220 \times 6} = \frac{400 \times 10^3}{141 + 2880} \approx 132\ (days)$$

Thus, the maximum node lifetime is 132 days, and the power consumption for host MCU and other peripheral hardware devices have not been included.

Scenario 2 is made based on such assumptions:

1. The system is implemented in the continuous scanning mode with event-driven model;
2. Only one remote node: a wireless joystick is deployed in the network, thus the continuous scanning mode can be applied in the active mode, without considering channel timing control;

3. The daily usage for each remote node is 6-hour operations in the active mode, 6 hours in the idle mode and 12 hours in the parking mode. The power management for idle mode and parking mode are the same in this scenario;
4. Assume that the incoming event on the joystick is detected with Poison distribution, and the average inter-arrival rate λ is assumed to 2 Hz in the active mode;
5. The probability α is set to 1 indicating that every collected data message will be sent to the central hub node;
6. The retransmission rate ρ is 0 since only one remote node is operated in the network, no channel collision or overlap will occur, therefore the remote node will return to the initial state without having to listen to the channel after each transmission;
7. The remote nodes operate in the shared channel mode in active mode;
8. The remote node is powered by two CR2032 coin cell batteries, which provide a capacity of 400 mAh in total.

The average current consumption in the active mode can be computed by applying Equation (7):

$$\begin{aligned} & \mathrm{I}_{\text{average}} \\ &= \frac{\mathrm{I}_{\text{idle}} + \lambda\left[I_{open}t_{open} + I_{close}t_{close} + I_{Tx}t_{Tx} + t_{tx_{completed}}I_{tx_{completed}} + 3t_{cmd_{msg}}I_{cmd_{mesg}}\right]}{\left[1 + \lambda\left[t_{open} + t_{close} + t_{Tx} + t_{tx_{completed}} + 3t_{cmd_{msg}}\right)\right]} \\ &= \frac{2 + 2 \times (65928 + 1304 + 30600) \times 10^{-3}}{1 + 2 \times (5.5 + 8.2 + 2.7 + 0.23 + 3 \times 2.4) \times 10^{-3}} \approx 198\ \mu A \end{aligned}$$

In the idle mode, the remote node will keep all its channels closed and not to response any RF message until an incoming event is detected. Thus, the average current consumption is 2 μA.

The node lifetime can be estimated by:

$$\frac{400 \times 10^3}{11.78 \times 12 + 2 \times 6 + 198\ \times 6} = \frac{400 \times 10^3}{153 + 1188} \approx 298(days)$$

Compared with the average current consumption for operations in active mode in the shared channel mode with 8Hz message rate, the result shows that the current consumption for operations in the continuous scanning mode with 2 Hz inter-event rate will not decrease significantly. The average current consumption in the active mode is 260 μA with the schedule-driven mode and 198 μA with the event-driven mode. This is because even the power cost for message reception is eliminated in the continuous scanning mode, the power cost for switching the channel ON and OFF takes a large proportion of the total power consumption. However, the remote node does not have to listen to the channel during the idle mode in the continuous scanning mode. In the idle mode, the remote node has to receive addressing messages from

the hub node to maintain channel synchronization. It consumes average current of 220 μA. With event-driven mode, the remote node will simply close all the channels when it does not wish to send data messages to the hub. The average current consumption is 2μA, which is the current consumption in the idle state from the data sheet [88]. This will significantly conserve power consumption and result in a longer node lifetime for operations with the event-driven mode.

However, in the second scenario, only one remote node is operated in the network. The retransmission rate has not been taken into account. For implementing multiple remote nodes with the event-driven mode, the channel collision and the channel overlap may occur frequently, which will increase the average current consumption. More studies will be required to investigate the relationship between the number of remote nodes and the retransmission rate.

5.7 Summary

ANT protocol is a light-weight protocol with low communication overheads which is designated for low-power, short-range wireless communications. A power management module is developed based upon ANT protocol for a particular application: wireless control on a power wheelchair. The primary principles applied in developing the power management module include:

1) The power states and state transitions are controlled by one hub node, as it is the only one designed for the access of user interface. All the user controls over the entire network must be achieved through the hub node. This means that a remote node has to perform auto device pairing to engage it into the network again once it loses connection with the hub node.
2) The power management should features ease of control, so that the handicapped user is able to gain full control over the system.
3) It should utilize the power states and state transitions provided by ANT protocol whenever possible to simplify the development of the power management.
4) The power management module should be compatible with the auto device pairing procedure.

This thesis presents an infrastructural with proposed power management module for ease of future development. The current consumption for ANT has been tested and measured under different power states, and the state transitions of ANT have been implemented. However, the power states and state transitions for host MCU and other peripheral hardware devices are not involved in this thesis and require more research work.

Chapter 6 Conclusions and Future Work

This thesis has presented system architecture for wireless sensing and control particularly on a power wheelchair, and the platform built could be potentially applied to many other automotive devices. By utilizing a hybrid network, the architecture is able to support fast, flexible system self-construction and easy access to power management. This architecture has been developed and validated through development of an ANT+ core wireless platform. The development procedure includes:

1. Selection of a commercial wireless protocol which suits the applications in WSN on a power wheelchair. ANT+ protocol is selected due to its light-weight and ultra-low power. Other protocols such as ZigBee and Bluetooth have been investigated in terms of flexibility, power-efficiency and cost.

2. Hardware design of a prototype to demonstrate the proposed development. We have developed a prototype which provides functionalities required to implement WSN protocols and applications demonstration on the power wheelchair. The prototype board provides ANT+ transceiver, host MCU and user interface. Two full version boards were made as the hub node and four cut-down version boards for the remote node applications. Two different versions of hardware prototype are designed. The full-version prototype offers more input interface, and is equipped with an external power supply socket to power the PCB while programming and debugging the host MCU. And the cut-down version only provides essential components for testing purpose.

3. We have presented an auto device pairing mechanism which provides fast and reliable network self-construction and self-maintenance. The auto device pairing provides a straightforward way to allow users to add devices into or take devices out of the wheelchair without any explicit instructions. The auto device pairing mechanism takes advantages of ANT+ protocol and utilizes handshaking procedures so that users are able to gain full control over the system via the hub node. We have validated that the hub is able to perform multiple tasks through auto device pairing mechanisms and we have identified initial configurations for implementing the auto device pairing successfully.

4. A device localization approach is suggested in this thesis to support the auto device pairing while multiple identical devices needs to be deployed into the network in different locations. Several different device localization methods have been presented and analyzed in this thesis, and it requires further research to determine a comprehensive solution while the development is advanced into industrial phase.

5. In addition to network self-construction and maintenance, we have also presented power management based upon ANT+ core wireless platform for optimizing the power consumption of remote node which is tightly power constrained. In this thesis, power management focuses on application layer and system level. It allows the entire system to dynamically transverse through different power states by accessing the user interface on the hub node. The power management module in this thesis aims to satisfy the requirements of a particular application. However, it can be considered as a platform for future developments to be expanded into larger application domains. A novel approach, master-slave-swap operation is developed, to take advantages from the shared channel mode (e.g. precise channel management) and the continuous scanning mode (e.g. less power consumption). This method allows a remote node to dynamically transverse through both modes depending on the status of the system.

6. A node lifetime estimator has been modeled in Matlab platform to help developers improve efficiency or provide insight into how the system operates in different scenarios. Some measurements have been taken in laboratory, and put into the mathematical model to estimate the node lifetime in different scenarios.

To validate our auto device pairing presented. We evaluated it with a demonstration on a power wheelchair by interfacing our development board with a DX module for steering wheelchair wirelessly as shown in Figure 6-1. It took approximately 2 ~ 3 seconds for the initial device pairing and then the hub node will receive RF signals from the remote node wirelessly and an interface board (the yellow board) transfers RF signals into control command messages to drive the wheelchair.

Figure 6-1 Demonstration on a power wheelchair.

Note that the auto device pairing is only implemented to assign device configurations for network integration and channel configurations for building a wireless link while a new device needs to be engaged into a network. All configurations will be stored into memory of host MCU for quick system startup once a remote node has been registered into the network. This pairing mechanism features ease of implementation. However, it lacks security access.

The device localization methodologies have been proposed in this thesis. However, as the demonstration in this thesis is performed only with a peer-to-peer communication between one master node and one slave node, it is not required for the hub node to obtain the physical

topology information to construct the network. The device localization is demonstrated in this project.

A power management module is developed and demonstrated. This enables a wireless network to dynamically transition between four power modes to optimize the power efficiency. A hub node connected to the wired backbone is able to determine the transitions according to the status of the system. This offers a great advantage for the ease of control.

The power measurements have been obtained by reading the voltage across a shunt resistor. ANT protocol data sheet has claimed its ultra-low power, allowing up to years node lifetime. However, it highly depends on the usage and the application, and developers can utilize the power estimator to figure out the node lifetime in different scenarios.

The development offers an infrastructure for utilizing wireless technologies to achieve autonomous control for sensing and control functionalities over a power wheelchair. This enables the future developments of power wheelchair system to take advantages from many aspects. However, many research topics arise from the development of this project and considered to be future work. These topics can be categorized into two groups: ID management module and power management module.

For ID management module, we have proposed a solution for auto device pairing. However, such a method has not been tested with a large number of remote nodes. Some potential problems may be encountered when the number of remote nodes increases, as the hub has to perform at very high message rate to maintain large number of wireless links in polling cycle. It is suggested to operate ANT protocol in default message rate (~4 Hz), and the system may become instable with high message rate.

On the other hand, the system latency may increase with number of remote nodes, as the time period of one polling cycle will increase with more remote nodes. To tackle latency problem due to a large number of remote nodes, a decentralized structure which employs multiple hub nodes can be considered for future development.

In this project, the auto device pairing is implemented by a serial of handshaking procedure in a public wireless environment. It lacks of security control. For future development, if high security level is required for device pairing for the applications on a power wheelchair, a seeing-is-believing methodology can be applied by equipping each remote node with a device for reading the link key. An example can be found in [80], which is an application of wireless home automation system which is shown in Figure 6-2. A simple swipe on a slot enables remote nodes read link key of the network from the hub node and offer high level of security for network construction. This may be one option for future development if some devices requiring high level of security to protect private information.

Figure 6-2 Installation devices by Homekey Swipe.

As for successfully accomplishing the auto device pairing, the hub requires information of the number of remote nodes and log-in table. If up-to-date device which has not been registered in the log-in table in the hub, it requires reconfiguration of the hub. This can be processed by connecting the hub node to the PC. However, for future vision, a wireless hand held programmer (HHP) is proposed to offer a complete wireless solution.

The primary intention for this project is to provide a platform for future development. Thus, in this thesis, it only provides a basic module of the power management and a node lifetime estimator for further studies. More research work is required to complete the power management for optimizing the power efficiency.

1. The continuous scanning mode is potentially applied for operations in active mode theoretically. In active node, the remote node sends an information message which contains data it collects from the environment or the users. In the shared channel mode, the transmission is controlled by the hub node. The remote node can only send the message while it receives an addressing message from the hub. In the continuous scanning mode, the remote node can send the information message whenever available. However, a channel management needs to be developed for allocating transmission of each remote node into individual time slot. This could be complex especially for a large network. In this project, the shared channel mode is utilized for operations in active mode for the ease of channel management of the share channel mode.
2. In this project, nRF24AP2 chipset is utilized for development and testing. It is a drop-in module with ANT+ core. It eases burden of development from intensive hardware and antenna design. However, it contains peripheral hardware that may not be required for the applications on wireless control over a power wheelchair. The block diagram of internal circuitry is shown in Figure 6-3. According to the block diagram of internal circuitry, we can design an on-board RF transceiver instead of a drop-in module to integrate it into the hardware layout of wireless nodes. It benefits from minimizing the peripheral devices and optimizing the layout of the circuitry. ANT has already provided chip-based solution which is based on nRF24L01+ radio platform [97]. However, it imposes the burden for extensive RF and antenna design.

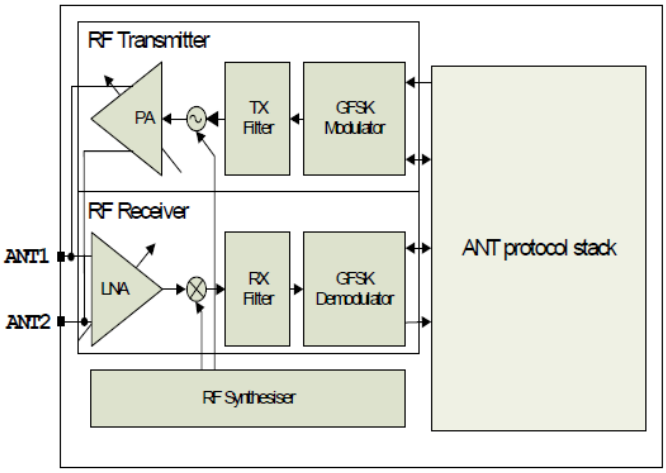


Figure 6-3 Internal circuitry of ANT+ platform.

3. ANT protocol provides transmission power selection feature, offering four transmit power level for a specified channel: -20 dBm, -10 dBm, -5 dBm and 0 dBm. Higher power levels increases current consumption, but offers higher level of signal-to-noise ratio (SNR) and thus enhancing the signal integrity. This provides ANT node flexibility to automatically select the appropriate power level dynamically according to the noise level of the environment to optimize the power consumption without sacrificing the channel reliability and signal integrity. However, it requires developers to implement experiments in various noise environments to determine the most appropriate power levels for different noise levels. And note that high power level may have RF certification implications, it is important to ensure that the selected power level meets the regulatory requirements of the region of intended sale.
4. This project is developed based upon a COTS RF platform, and it eases the development from intensive protocol design. However, the power management is tightly constrained by the OSI layer model of ANT protocol, only the high-level layers are user-defined, low-level layers are implemented by ANT. For example, the protocol does not support variable length of data message. Thus, power management development in this project focuses on application layer and system level. Lots of mainstream research such as medium access control, cross-layer protocol optimization, data aggregation for increasing power efficiency cannot be applied. If developers gain access to manipulate on low-level layers or select wireless protocol with larger flexibility, lots of power management approaches in the literature can be incorporated into the wireless platform developed in this project to enhance the performance.

For several years, lots of research work has been conducted to expose possible application scenarios for WSN. The system architecture presented in this thesis is ready to achieve some commercial usage. The first stage of WSN will likely to be applied for non-mission critical application scenarios, for example, a wireless joystick may be the first commercial product

based on the architecture presented in this thesis. Additionally, high-rate, mission-critical applications such as wireless collision avoidance system will become a reality in the near future. Such applications demand extremely high levels of reliability and predictability. Failures in a security or control system may lead to injury to personnel or even more. These systems must be tested and validated in many different extreme environments for years before they can be trusted.

The applications of environmental controls can be integrated into the wireless platform on the wheelchair to benefit handicapped from gaining access to control door, window, curtain and etc. This will offer a comprehensive solution by simply integrating more functionality into one wireless platform with ease of operation and cost efficiency.

While the system presented in this thesis is targeted to meet the demands of real-world commercial applications, the enabling technologies in wireless communication such as CMOS processes and RF technology will continuously evolve. The node lifetime will improve with the emerging technology. Currently, technology allows multi-year usage with a single pair of AA batteries. The upcoming technology will be applied to decrease the power consumption, reduce the physical size of energy storage devices and lower the cost of wireless platform. With the advances in semiconductor and RF technologies, industry will benefit from wireless technology from reduced power consumption, ease of deployment, flexibility and low cost.

REFERENCE

[1] Y. Ko and N. H. Vaidya. “Location-Aided Routing (LAR) in Mobile Ad Hoc Networks,” *Wireless Networks*, vol. 6(4), pp. 307-321, July, 2000.

[2] W.-H. Liao, Y.-C. Tseng, and J.-P. Sheu, “GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks,” *Telecommunication Systems*, vol. 18(1), pp. 37-60, 2001.

[3] F. Kuhn, R. Wattenhofer, Y. Zhang, and A. Zollinger, “Geometric Ad-Hoc Routing: Of Theory and Practice,” in Proc. of *ACM PODC’03*, pp. 63-72, 2003.

[4] Y. Ko and N. Vaidya, “Geocasting in Mobile Ad Hoc Networks: Location-Based Multicast Algorithms,” in Proc. of *IEEE WMCSA’99*, pp. 101, 1999.

[5] W.-H. Liao, Y.-C. Tseng, K.-L. Lo, and J.-P. Sheu. “Geogrid: A Geocasting Protocol for Mobile Ad Hoc Networks Based on Grid,” *Journal of Internet Technology*, vol. 1(2), pp. 23-32, 2000.

[6] M. Mauve, H. Fuler, J. Widmer, and T. Lang. “Position-Based Multicast Routing for Mobile Ad-Hoc Networks,” *Technical Report TR-03-004, Department of Computer Science, University of Mannheim*, 2003.

[7] Y.-C. Hu, A, Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks,” in Proc. of *INFOCOM’03*, vol. 3, pp. 1976-1986, April 2003.

[8] Y. Xu, J. Heidemann, and D. Estrin, “Geography-Informed Energy Conservation for Adhoc Routing,” in Proc. of *ACM/IEEE MOBICOM’01*, pp. 70-84, 2001.

[9] Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang, “Serial hook-ups: a comparative usability study of secure device pairing methods,” In *SOUPS ’09: Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, New York, NY, USA, 2009. ACM.

[10] K. Hinckley. “Synchronous gestures for multiple persons and computers.” In *Proc. UIST 2003*, pages 149–158. ACM Press, 2003.

[11] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, “Smart-Its Friends: A technique for users to easily establish connections between smart artefacts,” In *Proc. UbiComp 2001*, pages 116–122. Springer-Verlag, 2001

[12] J. Rekimoto, Y. Ayatsuka, M. Kohno, and H. Oba, "Proximal interactions: A direct manipulation technique for wireless networking," In *Proc. INTERACT 2003*, pages 511–518. IOS Press, 2003.

[13] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for WSNs," In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, 2004.

[14] T. Kindberg and K. Zhang, "Validating and securing spontaneous associations between wireless devices," In *Proc. ISC 2003*, pages 44–53, 2003.

[15] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," In *Proc. 7th International Workshop on Security Protocols*, pages 172–194. Springer-Verlag, 1999.

[16] Liang Cai, Kai Zeng, Hao Chen, and Prasant Mohapatra. "Good Neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas." In *Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 6-9, 2011.

[17] Frank Stajano and Ross Anderson, "The resurrecting duckling: Security issues for ubiquitous computing," (supplement to computer magazine). *Computer*, 35:22–26, 2002.

[18] J.M. McCune, A. Perrig, M.K. Reiter, Seeing-is-believing: Using camera phones for human-verifiable authentication, in: IEEE Symposium on Security and Privacy, 2005.

[19] R. Chang and V. Shmatikov, "Formal Analysis of Authentication in Bluetooth Device Pairing," In 1st International Symposium on Leveraging Applications of Formal Methods (ISOLA04), 2007.

[20] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, Narayan Mandayam, "ProxiMate: Proximity-based Secure Pairing using Ambient Wireless Signals", *Ninth Annual International Conference on Mobile Systems, Applications, and Services (MobiSys 2011), Washington D.C., USA, 2011*

[21] Arun Kumar, Nitesh Saxena, Gene Tsudik, Ersin Uzun , "A comparative study of secure device pairing methods", Pervasive and Mobile Computing - PerCom , vol. 5, no. 6, pp. 734-749, 2009

[22] Chong, Ming Ki and Gellersen, Hans, "How Users Associate Wireless Devices." In: CHI2011, 07-12 May 2011, Vancouver BC, Canada.

[23] T.S Rappaport, "Wireless communications –Principles and practice", 2nd Edition, Prentice Hall, 2001.

[24] L. Doherty, K. Pister, and L. Ghaoui, "Convex position estimation in WSNs," In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, 2001.

[25] B. Parkinson and J. Spilker, “Global positioning system: theory and applications,” *Progress in Aeronautics and Astronautics*, 1996.

[26] N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less low cost outdoor localization for very small devices,” *IEEE Personal Communications Magazine*, October 2000.

[27] T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, “Range-Free localization schemes in large scale sensor networks, ” In *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2003.

[28] D. Niculescu and B. Nath, “DV-based positioning in ad-hoc networks,” *Telecommunication Systems*, 2003.

[29] Christopher Jerry Mallery, “Location and Topology Discovery in WSN”, Ph.D. dissertation, Computer Science, Washington State University, Pullman, WA, 2009

[30] C. SAVARESE, J.M.Rabaey, J. BETUEL “Locationing in Distributed Ad-Hoc WSNs,”*2001 IEEE International Conference on, Vol. 4 (2001), pp. 2037-2040.*

[31] L. Luo and A.S. Sethi, "Topology Discovery in Wireless Ad Hoc Networks." Proc. SCI-2005, 9th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, FL (July 2005), pp. 86-91.

[32] R. Stoleru, J. Stankovic, S. Son, “Robust Node Localization for WSNs,” *Emnets*, June 2007.

[33] MayWong and Demet Aksoy, “Relative accuracy based location estimation in wireless ad hoc sensor networks,” In *Proceedings of the IEEE International Conference on Communications (ICC 2007)*, pages 3244–3250, Glasgow, U.K., June 2007.

[34] Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E, “A Survey on Sensor Networks,” IEEE Communications Magazine, August 2002, pp.102-114.

[35] Priyantha, N.B., Chakraborty A., Balakrishnan H, “The Cricket Location-Support System,” Proc. ACM Int. Conf. on Mobile Computing and Networking, August, 2000.

[36] Niculescu D., Nath B, “Error Characteristics of Ad Hoc Positioning Systems (APS),” Proc. ACM Int Symp on Mobile Ad Hoc Networking and Computing, 2004.

[37] A. Savvides, C.C. Han and M.B. Srivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors,” in: *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom)*, Rome, Italy (July 2001) pp. 166–179.

[38] Lazos L., Poovendran R, “SeRLoc: Secure Range-Independent Localization for WSNs,” Proc. of ACM Workshop on Wireless Security, 2004.

[39]ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.9-18.

[40] ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.27.

[41] ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.39 - 44.

[42] Auto Shared Channel – Master Example, Rev1.4, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.8.

[43] Chong Hui Kim, Seong Jin Kim, Hyun Sang Kim,and Byung Kook Kim, “Development of autonomous robotic wheelchair system for the motor-disabled,” *International Conference on Aging, Disability, and Independence*, pp. 214-215, 2006

[44] Kim J, Cho S, Kim S J, “Preliminary Studies to Develop a Ubiquitous Computing and Health-monitoring System for Wheelchair Users", BodyNets, Tempe, AZ, March, 2008.

[45] Carlos F. García-Hernández, "*WSNs and Applications: a Survey*", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.

[46] José A. Gutierrez, Marco Naeve, Ed Callaway, Monique Bourgeois, Vinay Mitter, Bob Heile, “IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks”; *IEEE Network*, pp. 12-19, September/October 2001.

[47] Chien-Chung Shen, Chavalit Srisathapornphat, Chaiporn Jaikaeo; “Sensor Information Networking Architecture and Applications”; *IEEE Personal Communications*, pp. 52-59, August 2001.

[48] Elaine Shi, Adrian Perrig; “Designing Secure Sensor Networks”; *IEEE Wireless Communications*, pp. 38-43, December 2004.

[49] Sarjoun S. Doumit, Dharma P. Agrawal; “Self-Organizing and Energy-Efficient Network of Sensors”; IEEE, pp. 1-6, 2002.

[50] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci; “A Survey on Sensor Networks”; *IEEE Communications Magazine*, pp. 102-114, August 2002.

[51] Nirupama Bulusu, John Heidemann, Deborah Estrin; “GPS-less Low-Cost Outdoor Localization for Very Small Devices”; *IEEE Personal Communications*, pp. 28-34, October 2000.

[52] Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile, Venkat Bahl, “Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks”; *IEEE Communications Magazine*, pp. 70-77, August 2002.

[53] Kay Romer, Friedemann Mattern; “The Design Space of WSNs”; *IEEE Wireless Communications*, pp. 54-61, December 2004.

[54] Wendi B. Heinzelman, Amy L. Murphy, Hervaldo S. Carvalho, Mark A. Perillo; “Middleware to Support Sensor Network Applications”; *IEEE Network*, pp. 6-14, January/February 2004.

[55] Jason Lester Hill; “System Architecture for WSNs,” PhD thesis, University of California, Berkeley, 2003.

[56] http://en.wikibooks.org/wiki/Communication_Networks/Network_Topologies

[57] Hubert Zimmermann, “OSI reference model,” *IEEE Transactions on Communications* **COMM-28** (4) (1980), p. 425.

[58] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive protocols for information dissemination in WSNs,” MobiCOM '99, pp. 174-185, Seattle, WA, 1999.

[59] Meng Zheng, Wei Liang, Haibin Yu, Yang Xiao, “Cross Layer Optimization for Energy-Constrained WSNs: Joint Rate Control and Routing,” Comput. J. 53(10): 1632-1642, 2010

[60] I.F. Akyildiz, W. Su, “A power aware enhanced routing (PAER) protocol for sensor networks,” Georgia Tech Technical Report, January 2002, submitted for publication.

[61] Vuran M.C., Akan O.B., Akyildiz I.F., "Spatio-Temporal Correlation: Theory and Applications WSNs," Computer Networks Journal (Elsevier Science), vol. 45, no. 3, pp. 245 -259, June 2004.

[62] Akyildiz I.F., Vuran M.C., Akan O.B., "On Exploiting Spatial and Temporal Correlation in WSNs," in Proc. WiOpt'04: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, pp. 71 -80, March 2004.

[63] Akan, O.B., and Akyildiz, I.F., ``Event-to-Sink Reliable Transport in WSNs,'' to appear in IEEE/ACM Transactions on Networking, October 2005

[64] Sankarasubramaniam, Y., Akan, O.B., and Akyildiz, I.F., "ESRT: Event-to-Sink Reliable Transport in WSNs," in Proc. ACM MobiHoc'03, Annapolis, Maryland, USA, June 2003.

[65] Melodia, T., Pompili, D., and Akyildiz, I.F., "Optimal Local Topology Knowledge for Energy Efficient Geographical Routing in Sensor Networks,'' in Proc. of IEEE Infocom 2004, Hong Kong, P.R. China, March 2004.

[66] Melodia, T., Pompili, D., and Akyildiz, I.F., "On the Interdependence of Distributed Topology Control and Geographical Routing in Ad Hoc and Sensor Networks,'' to appear on JSAC Special Issue on Wireless Ad Hoc Networks, March 2005.

[67] Sankarasubramaniam, Y., Akyildiz, I.F., and McLaughlin, S.W., "Energy Efficiency based Packet Size Optimization in WSNs," in Proc. First IEEE International Workshop on Sensor Networks Protocols and Applications (SNPA'03), Anchorage, Alaska, USA, May 2003 (held in conjunction with ICC'03).

[68] Su, W. and Akyildiz, I. F., "Time-Diffusion Synchronization Protocol for Sensor Networks," to appear in IEEE/ACM Transactions on Networking, Feb. 2005.

[69] Wei Ye, John Heidemann and Deborah Estrin, “An Energy-Efficient MAC Protocol for WSNs,” In Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), New York, NY, USA, June, 2002

[70] Jeremy Elson and Deborah Estrin, “Time Synchronization for WSNs,” In Proceedings of the 2001 International Parallel and Distributed Processing Symposium (IPDPS), Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001, San Francisco, CA, USA

[71] Chalermek Intanagonwiwat, Ramesh Govindan and Deborah Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” *In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM '00), August 2000, Boston, Massachussetts*

[72] Deborah Estrin , John Heidemann , Ramesh Govindan and Satish Kumar, “Next Century Challenges: Scalable Coordination in Sensor Networks,” *In Proceedings of the Fifth Annual International Conference on Mobile Computing and Networks (MobiCOM '99), August 1999, Seattle, Washington.*

[73] Ya Xu, John Heidemann and Deborah Estrin, “Adaptive Energy-Conserving Routing for Multihop Ad Hoc Networks,” Research Report 527, USC/Information Sciences Institute, October 2000

[74] W.R. Heinzelman, J. Kulik, H. Balakrishnan, “Adaptive protocols for information dissemination in WSNs,” Proceedings of the ACM MobiCom’99, Seattle, Washington, 1999, pp. 174–185.

[75] M. Perillo and W. Heinzelman, "WSN Protocols,'' *Fundamental Algorithms and Protocols for Wireless and Mobile Networks*, CRC Hall, 2005.

[76] J. Yick, B. Mukherjee, and D. Ghosal, “WSN survey”, Computer Networks, Vol. 52, Issue 12, pp. 2292-2330, August 2008

[77] A. Bharathidasan and V. A. S. Ponduru, "Sensor networks: an overview", Potentials, IEEE Volume 22, Issue 2. 2003.pp.20 –23.

[78] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks,” *IEEE Communications Magazine*, Aug. 2002.

[79] Bob Heile, "Wireless Sensors and Control Networks: Enabling New Opportunities", Available at http://www.zigbee.org

[80] http://www.hometoys.com/ezine/08.12/heartbeat/

[81] Wang, Y., Swartz, R.A., Lynch, J.P., Law, K.H. and Loh, C.-H. (2007). "Performance evaluation of decentralized wireless sensing and control in civil structures," Proceedings of SPIE 14th International Symposium on Smart Structures and Materials & Nondestructive Evaluation and Health Monitoring, 6531: 653113, San Diego, CA, March 18 - 22, 2007

[82] Chee-Yee Chong; Kumar, S.P., "Sensor networks: Evolution, opportunities, and challenges," *Proc. IEEE*, August 2003.

[83] *Proceedings of the Distributed Sensor Nets Workshop*. Pittsburgh, PA: Dept. Comput. Sci., Carnegie Mellon Univ., 1978.

[84] R. Rashid and G. Robertson, “Accent: A communication oriented network operating system kernel,” in *Proc. 8th Symp. Operating System Principles*, 1981, pp. 64–75.

[85] C. Myers, A. Oppenheim, R. Davis, and W. Dove, “Knowledgebased speech analysis and enhancement,” presented at the Int. Conf. Acoustics, Speech and Signal Processing, San Diego, CA, 1984.

[86] S. Kumar and D. Shepherd, “SensIT: Sensor information technology for the warfighter,” in *Proc. 4th Int. Conf. on Information Fusion*, 2001, pp. TuC1-3–TuC1-9.

[87] J. M. Kahn, R. H. Katz, and K. S. J. Pister, “Mobile networking for smart dust,” in *Proc. ACM/IEEE Int. Conf. Mobile Computing and Networking (MobiCom)*, 1999, pp. 271–278.

[88] Power States, Rev.1.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.5-6.

[89]ANT AP2 Transceiver Module Datasheet Rev.1.7, Dynastream Innovations Inc, Alberta, Canada, 2011, pp. 7-10.

[90]nRF24AP2 Product Specification Rev.1.2, Dynastream Innovations Inc, Alberta, Canada, 2010, pp. 23-33

[91]Interfacing with ANT General Purpose Chipsets and Modules Rev.2.1, Dynastream Innovations Inc, Alberta, Canada, 2010, pp. 5-20

[92] nRF24AP2 Product Specification Rev.1.2, Dynastream Innovations Inc, Alberta, Canada, 2010, pp. 43-45

[93] ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.21-22.

[94] ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.10-17.

[95] http://www.thisisant.com/pages/products/ap2-module

[96] John H. Davis, “Functions, Interrupts, and Low-Power Modes” in MSP430 Microcontroller Basics, Burlington, MA: Newnes, 2008, pp.198-205.

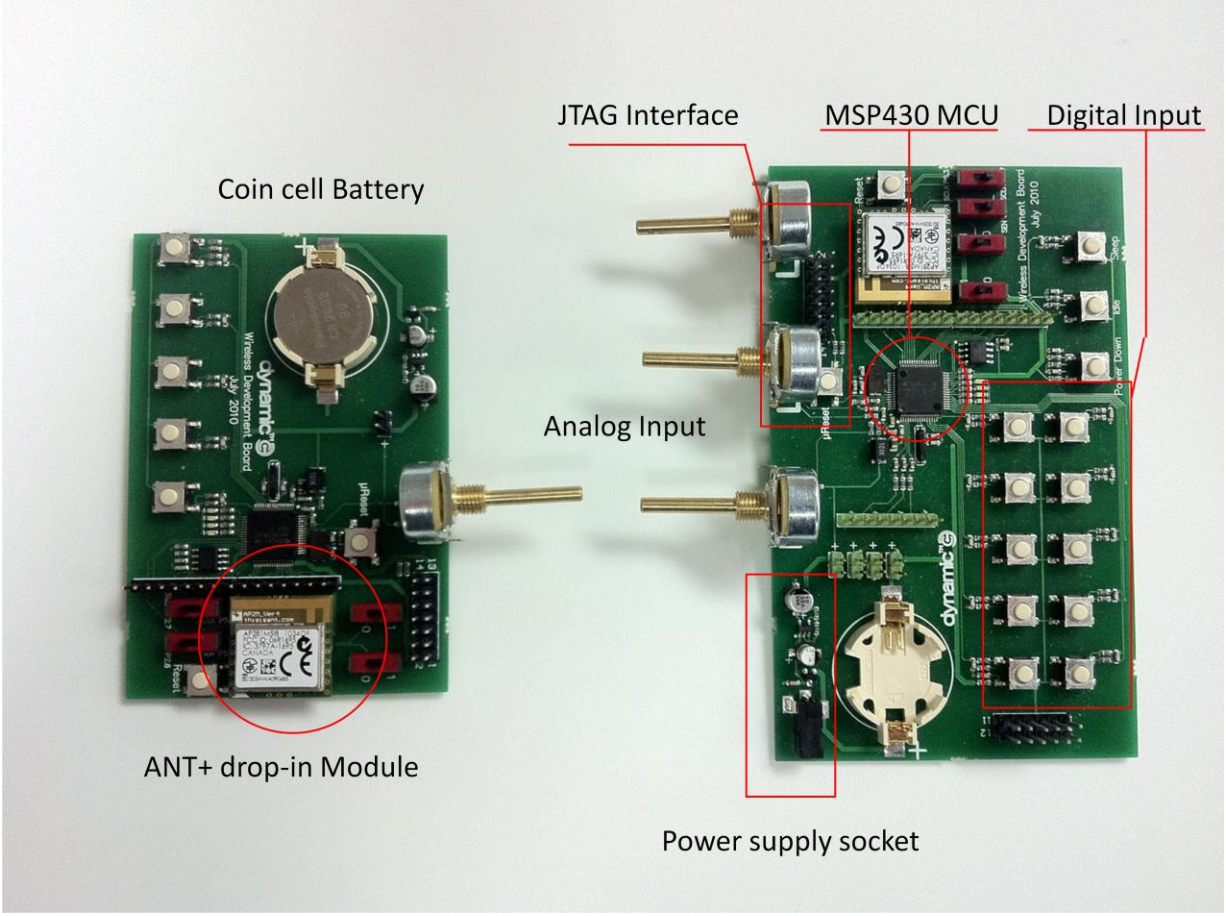
[97] http://www.thisisant.com/pages/products/nrf24ap2

[98] Lajara, Rafael; Pelegrí-Sebastiá, José; Solano, Juan J. Perez. 2010. "Power Consumption Analysis of Operating Systems for WSNs." *Sensors* 10, no. 6: 5809-5826

[99] Nandini Patil, P. R. Patil, “Data aggregation in WSN”, International journal of service computing and computational intelligence, ISSN 2162-514X

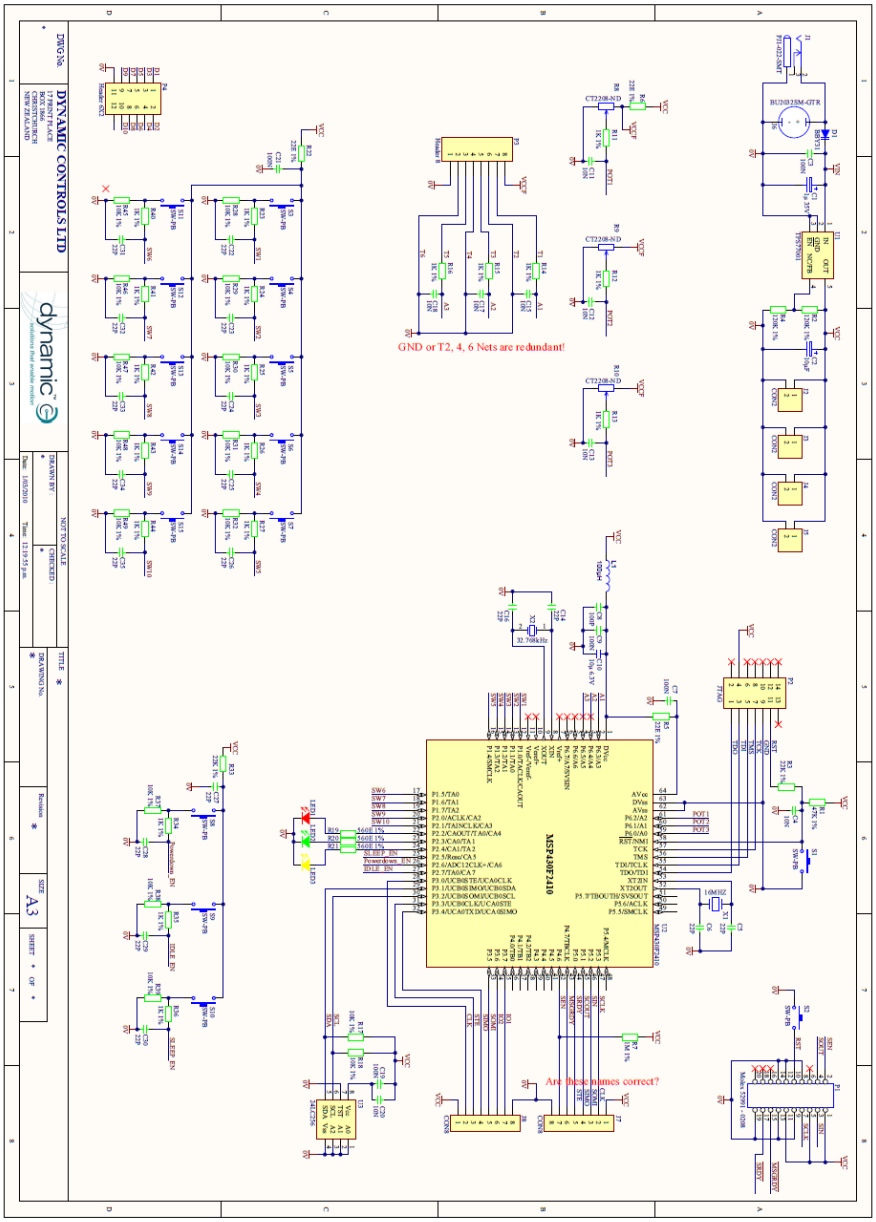
[100] ANT Message Protocol and Usage, Rev.3.1, Dynastream Innovations Inc, Alberta, Canada, 2009, pp.71-73.

Appendix A: **HARDWAER PROTOTYPE**



The larger board on the right hand side is a full-version prototype which offers more input interface, and equipped with an external power supply socket to power the PCB while programming and debugging. The small one on the left is a cut-down version prototype, which provides only essential components for testing purpose. The dip-switch allows developers to switch the drop-in module between synchronous mode and asynchronous mode.

Appendix B: **PCB SCHEMATIC**



Appendix C: PCB LAYOUT